Canada Border Services Agency | Agence des services frontaliers du Canada



# CBSA Security Program Management Framework

PROTECTION • SERVICE • INTEGRITY





# Table of Contents

Canada Border Services Agency | Agence des services frontaliers du Canada



# Security Program Management Framework

## 1. Purpose

The purpose of this framework is to identify all the Policy on Government Security (PGS) program requirements that impact the Canada Border Services Agency (CBSA) and detail all CBSA Security Program related accountabilities, roles and responsibilities, as well as the direction in which security management and governance is structured Agency-wide. This ensures that CBSA employees and managers at all levels effectively manage security risks, protect information, assets and people to ensure the continuity of services and operations available to the Canadian public, while sustaining a low level of risk to other departments and to the government as a whole. This reflects principles of effective governance, risk management, planning, monitoring, evaluation, and continuous improvement.

This framework provides strategic guidance and direction on the design, development and implementation of the CBSA Security Program and its sub-programs. It establishes the required governance parameters as defined by legislation and policy.

This framework is supported by directives, standards, guidelines and procedures which provide subject-specific amplification. Please refer to the CBSA Security Volume for more information.

## 2. Effective Date

The Canada Border Services Agency (CBSA) Security Program Management Framework is effective as of January 23, 2015.

## 3. Application

This framework and its supporting documentation apply throughout the entire CBSA. This includes:

- all properties, facilities and assets (including information);
- all CBSA employees (permanent, term, casual, and part-time), contract and private agency personnel, and to individuals seconded or assigned to CBSA (including students); and
- visitors, volunteers and any person physically situated on or within a CBSA facility or in a CBSA controlled area.

## 4. Context

Government security is the assurance that employees and assets are protected against injury. The extent to which government can ensure its own security directly affects its ability to ensure protection of key assets and the continued delivery of services that contribute to the health, safety, economic well-being and security of all Canadians.







In the Public Sector, security is tied directly to the Canadian public's confidence in the Government of Canada's ability to protect them, their belongings and their identity. The Government, in its day-to-day operations, will often directly interact with Canadians to provide them with the services to which they are entitled. To do this in an effective manner, the Government must accurately identify the individuals or institutions with which it interacts. This results in the storage and manipulation of large amounts of personal and corporate information that must remain confidential at all times and be accessed only on a need-to-know basis. Public servants who have access to government information, assets and services must be trustworthy, reliable and loyal. Consequently, a broad range of government activities, from safeguarding information and assets, to delivering services, benefits and entitlements and responding to incidents and emergencies, rely upon this trust.

In the CBSA, the management of security is a living and dynamic process that requires the continuous assessment and proactive management of internal and external threats and their associated risks. It includes the implementation, monitoring and maintenance of appropriate internal management controls including: prevention (mitigation), detection, response and recovery. The management of security directly interacts with other management functions including access to information and privacy, risk management, emergency and business continuity management, human resources, occupational health and safety, real estate, material management, information management, information technology and finance. The management of security follows and adheres to the rules of natural justice and principles of procedural fairness to ensure the protection of individuals' rights. Security within the CBSA is most effective when it is integrated into the culture and day-to-day operations. Only in this way can the security program positively influence employees and management.

## 5. Authority

The authority for this framework is derived from the Section 7 of the *Financial Administration Act*, the Treasury Board of Canada Secretariat (TBS) Policy on Government Security (PGS), and the Directive on Departmental Security Management.

This document should be read in conjunction with related CBSA security directives, standards, guidelines and procedures as set out in the CBSA Security Volume and in periodic security bulletins and notices issued by the Departmental Security Officer (DSO). This framework will refer the reader to the additional resources as required. This framework, along with the other policy instruments can be referenced in the CBSA Security Volume.

## 6. Objective

The objective of this framework is to establish specific principles, set an integrated approach for managing the CBSA Security Program and identify all PGS security program requirements that impact the CBSA. This will achieve efficient, effective, and accountable management of security within the CBSA.







## 7. Expected Results

It is essential for the CBSA to have a cost effective and efficient security program in place to address the Agency's responsibilities towards the Canadian public and to ensure that the Agency remains compliant with the spirit, intent and mandated requirements of the Policy on Government Security (PGS), the Directive on Departmental Security Management, the Directive on Identity Management and all related standards.

The expected results of this framework include:

- Information, assets, services and employees are safeguarded from compromise and employees are protected against workplace violence;
- Clear identification of Agency-wide security related accountabilities and roles and responsibilities at both the individual and organizational levels;
- Establishment and maintenance of a culture of security within the Agency;
- Alignment of strategy, processes, and resources to maintain an effective and efficient security posture throughout the CBSA;
- Consistent security management practices supporting interoperability and information exchange in a secure and economically efficient manner;
- Active monitoring and reporting changes in the environment to ensure a timely response to existing and new threats, vulnerabilities and incidents;
- Continuity of government operations and services in the presence of security incidents, disruptions or emergencies;
- Effective management of security to ensure that CBSA does not unnecessarily increase risks to itself, other departments or to the government as a whole; and
- Governance structures, mechanisms and resources are in place to ensure effective and efficient management of security at both a departmental and government-wide level.

## 8. General Roles and Responsibilities

As specified in the following sections, CBSA Senior Management, the DSO, managers at all levels and employees are responsible for the implementation of security controls and the achievement of control objectives.

### President

The President has the overall responsibility for the effective implementation and governance of security and identity management within the Agency, while sharing the responsibility for the security of the Government as a whole. More specifically, the President's responsibilities include:

- Safeguarding CBSA employees and assets;
- Appointing a DSO;
- Implementing the PGS by supporting a security program that has a governance structure with clear accountabilities, thus effectively managing security within the Agency;





- Approving the CBSA Departmental Security Plan (DSP) that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving Agency security, while supporting its implementation;
- Ensuring that CBSA management at all levels identify and integrate security and identity management requirements into plans, programs, activities and services; and
- Ensuring appropriate remedial actions are taken to address issues regarding policy non-compliance, allegations of misconduct, suspected criminal activity or security incidents, including denying, revoking or suspending security clearances, as appropriate.

**Vice-President (VP) Comptrollership Branch**

The VP Comptrollership Branch provides overall functional direction within CBSA in regard to the Agency Security Program. The VP Comptrollership Branch presents security issues and interests to the President, Executive Vice-President (EVP) and Executive Committee in relation to security matters that have a substantial bearing upon the Agency's mission and obligations.

The VP Comptrollership Branch is responsible for ensuring that:

- The necessary security policies, procedures, and standards are established and integrated in the Agency Security Program;
- The appropriate and required resources (financial, human resources and assets) are allocated for the security program;
- The Security Program meets the President's performance expectations; and
- The appropriate monitoring and reporting of the program's performance are being completed.

**The Departmental Security Officer (DSO)**

The President of the CBSA has delegated the Director General, Security and Professional Standards Directorate, as the DSO to whom he has delegated the functional responsibility and authority for all aspects of the PGS except the authorities prescribed from being delegated as per the PGS.

The overall management of the security program can be summarized as follows:

- Establish and direct the Agency Security Program;
- Manage the relationships required to achieve the implementation of security requirements for all areas with security responsibilities;
- Ensure management, co-ordination and implementation of the requirements of all policy functions of the CBSA Security Program remain consistent with the PGS and its associated policy instruments;
- Ensure effective development, administration, risk management and monitoring of the Agency's security policies and programs;
- Ensure that Senior Management within the Agency are aware of their accountabilities and responsibilities pertaining to the Security Program and integrate them appropriately into their own policies, standards, guidelines, procedures and baselines;
- Ensure that accountabilities, delegations, reporting relationships and the responsibilities of Agency employees with security impacts are defined, documented and appropriately communicated;
- Provide functional direction, advice and guidance to the Agency's network of security practitioners;







- Foster a "culture of security" across the Agency; and
- Develop and deliver security awareness for employees and managers at all levels.

**The Chief Information Officer (CIO)**

The Vice-President, Information, Science and Technology Branch, is responsible for functioning as the Chief Information Officer for the Agency. The responsibilities of this position include:

- Ensuring the effective and efficient management of the Agency's information and IT assets;
- Ensuring appropriate security controls are applied to all Agency Information Technology (IT) and Information Management (IM) assets, activities and processes; and
- Ensuring a productive and functional relationship between the IT Security Coordinator (ITSC) and the DSO to ensure a coordinated and comprehensive approach to the implementation of Security Program requirements.

**Information Technology Security Coordinator (ITSC)**

The CBSA IT Security Coordinator has a functional reporting relationship to both the Chief Information Officer and the Departmental Security Officer.

The IT Security Coordinator's duties include:

- Establishing and managing the Agency IT security program as part of the overall coordinated departmental Security Program,
- Reviewing and recommending approval of IT security policies and standards, and all policies that have IT security implications,
- Ensuring review of the IT security related portions of Request for Proposals and other contracting documentation, including Security Requirements Checklists,
- Recommending approval of all contracts for external providers of IT security services,
- Working closely with program and service delivery managers to
  - ensure their IT security needs are met,
  - provide advice on safeguards,
  - advise them of potential impacts of new and existing threats, and
  - advise them on the residual risk of a program or service,
- Monitoring Agency compliance with Management of Information Technology Security (MITS) and associated IT security standards and guidance,
- Promoting IT security in the Agency,
- Establishing an effective process to manage IT security incidents, and monitor compliance with it, and
- Serving as the Agency's principal IT security contact.



**Executive Management**

Executive Management (Vice-Presidents, Executive Vice-President, and President) is responsible to:

- Set program objectives and provide oversight via the Executive Committee;
- Ensure the security of employees, assets, information and services;
- Ensure compliance with the Agency's security policy, standards and practices;
- Monitor adherence to the Agency's security policy, standards and practices within their areas of responsibility and report to the DSO any security incident or security breach;
- Implement program specific security requirements associated with their operational programs;
- Continuously encourage a "culture of security" across the Agency;
- Incorporate Security Program requirements when defining respective Agency priorities, strategic direction, program objectives, budget and allocations; and
- Approve all policy, standards and directives in conjunction with the DSO when a security element is involved.

**Managers at all levels**

Directors General, Directors, Managers and all other levels of management at headquarters and in the regions are responsible to:

- Apply security policies, standards, directives and guidelines within their respective areas of responsibility, and ensure understanding and compliance from all delegated employees;
- Ensure the protection of employees and the safeguarding of the information, assets and services for which they are responsible;
- Ensure security program requirements are integrated into business planning, programs, services and other management activities;
- Ensure the business continuity of respective areas of responsibility and ensure it conforms to the CBSA Business Continuity Program requirements;
- Assess security risks and periodically reassess and re-evaluate risks in light of changes to programs, activities or services, while taking corrective measures to address the identified deficiencies and strengthen the security posture of the Agency;
- Ensure that no individual is hired/appointed/acting or commences any work in a position without being screened and granted his or her required CBSA approved Security Level;
- Ensuring that a Security Briefing is provided to every employee upon hire;
- Ensure that they and their employees complete the mandatory online security awareness modules every two years;
- Monitor adherence to the Agency's security policies, directives, standards and practices within their area of responsibility;
- Report security incidents or breaches of security; and
- Monitor the implementation and effectiveness of security controls, and reporting to the DSO as appropriate.







**Employees at all levels**

All persons employed by the Agency (permanent, term, casual, and part-time), contract and private agency personnel, and to individuals seconded or assigned to CBSA (including students) are responsible to:

- Classify/designate and mark information they originate to ensure the appropriate safeguards are applied;
- Safeguard all information and assets under their control both onsite and offsite;
- Apply and follow physical security measures to control access to CBSA premises, information and assets;
- Apply security controls related to their area of responsibility to ensure that security requirements are integrated into day-to-day processes, practices and program delivery;
- Report security incidents through the appropriate channels and take direction from the DSO as appropriate;
- Maintain awareness of security concerns and issues to ensure their implications do not compromise the security posture of the Agency;
- Act in a manner both on and off-duty that would not reflect negatively on or compromise the integrity of the CBSA; and
- Complete the mandatory online security awareness module (every two years) or any other mandatory training related to sound security practices.

**Security Practitioners**

Persons responsible for coordinating, managing and providing advice and services related to the security activities that are part of a coordinated departmental security program, which include but are not limited to information security, information technology (IT) security, physical security, personnel security screening, emergency management, business continuity planning and regional security operations.

Security Practitioners in the CBSA are responsible to:

- Maintain a functional reporting relationship with the DSO through the appropriate functional authorities to ensure departmental security activities are coordinated and integrated;
- Select, implement and maintain security controls related to their area of responsibility to ensure that control objectives are achieved;
- Monitor and evaluate the implementation and effectiveness of security controls, report on the achievement of control objectives to the DSO, and recommend corrective action to address deficiencies identified through performance measurement activities and evaluations;
- Provide the DSO, managers at all levels and employees with advice on the application and effectiveness of security controls related to their area of responsibility;
- Support the DSO in the development and delivery of security awareness for employees and managers at all levels; and
- Participate in threat and risk assessments and contribute to the development of the Departmental Security Plan (DSP), as required.





## 9. Consequences

The President is responsible for ensuring appropriate remedial actions are taken to address issues regarding policy compliance, allegations of misconduct, suspected criminal activity or security incidents, including denying, revoking or suspending security clearances, as appropriate.

Consequences of non-compliance with the Agency's security policy instruments can include the following:

- Informal follow-ups, requests for internal-audit or formal direction on corrective measures; and
- Punitive or other administrative measures deemed appropriate in the circumstances imposed.

## 10. Appendices

Appendix A: Overview of the Security Program
Appendix B: CBSA Security Program Accountability Structure
Appendix C: Security Management Committee Terms of Reference

## 11. References

**Legislation relevant to this policy includes:**

Access to Information Act
Canada Evidence Act
Canada Labour Code
Canada Occupational Health and Safety Regulations
Canadian Charter of Rights and Freedoms
Canadian Human Rights Act
Canadian Security Intelligence Service Act
Charter of Rights and Freedoms
Customs Act
Criminal Code
Criminal Records Act:
Emergency Management Act
Financial Administration Act
Library and Archives of Canada Act
Privacy Act
Public Service Employment Act
Public Service Labour Relations Act
Royal Canadian Mounted Police Act
Security of Information Act
Youth Criminal Justice Act







**Treasury Board policies, directives and standards relevant to this policy include the following:**

Access to Information, Policy on
Directive on Departmental Security Management
Directive on Identity Management
Directive on Information Management Roles and Responsibilities
Fire Protection Standard
Government Security, Policy on
Information Management, Policy on
Framework for the Management of Risk
Internal Audit, Policy on
Internal Controls, Policy
Labour Relations, Policy on
Learning, Training, and Development, Policy on
Directive on Losses of Money or Property
Management of Information Technology, Policy on
Management of Materiel, Policy on
Management of Real Property, Policy on
Occupational Health and Safety, Policy on
Operational Security Standard—Business Continuity Planning (BCP) Program
Operational Security Standard on Physical Security
Operational Security Standard: Management of Information Technology Security (MITS)
Standard on Security Screening
Privacy Protection, Policy on
Policy on Management of Projects
Public Servants Disclosure Protection Act
Terms and Conditions of Employment, Directive on

**The following documents are also relevant to this policy:**
Values and Ethics Code for the Public Service
CBSA's Code of Conduct
Policy on the Disclosure of Customs Information (Section 107 of the Customs Act)
CBSA Security Volume

## 12. Policy Review

The Security Program Management Framework will be reviewed and revised, if required, annually to reflect program and organizational changes.

## 13. Enquiries

For more information please contact:

Security and Professional Standards Directorate
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca



# Appendix A: Overview of the CBSA Security Program

The CBSA Security Program is a complex entity which is responsible for all internal security services: personnel security, physical security, security in contracting, information security including communications security (COMSEC), information technology (IT) security, management of facilities that process special intelligence information, security policy development, program monitoring of security activities, professional standards investigations, business continuity management, emergency management, integrity risk assessment and integrity program guidance. The CBSA Security Program provides security services to approximately 13,000 Agency employees located at approximately 1,200 service points across Canada encompassing land, air, rail, marine ports, remote area border crossings and unmanned ports, mail centres, and in international locations.

The activities of the Security Program are governed by the Treasury Board Secretariat's Policy on Government Security (PGS), the Directive on Departmental Security Management (DDSM) and the Directive on Identity Management (DIM). Additional mandatory requirements are set out in standards which support the following subject areas: Information and Identity Assurance, individual security screening, Physical Security, Information Technology Security, Emergency and Business Continuity Management and Security in Contracting.

In the broadest context, government security is the assurance that employees and assets are protected against injury. The extent to which government can ensure its own security directly affects its ability to ensure protection of key assets and the continued delivery of services that contribute to the health, safety, economic well-being and security of all Canadians.

In the CBSA, the management of security is a living and dynamic process that requires the continuous assessment and proactive management of internal and external threats and their associated risks. It includes the implementation, monitoring and maintenance of appropriate internal management controls including: prevention (mitigation), detection, response and recovery. The management of security directly interacts with other management functions including access to information and privacy, risk management, emergency and business continuity management, human resources, occupational health and safety, real estate, material management, information management, information technology and finance. Security within the CBSA is most effective when it is integrated into the culture and day-to-day operations. Only in this way can the Security Program positively influence employees and management.

The requirements outlined in this framework form the basis for establishing effective security program management which enables the CBSA to meet all the security related requirements of the PGS, the associated directives and standards, in addressing its security program obligations.

The CBSA Security Program is supported by all branches within the Agency; however, it is administered by the Security and Professional Standards Directorate (SPSD) within the Comptrollership Branch. The President has designated the Director General of SPSD as the Departmental Security Officer (DSO) for the Agency to whom he has delegated the functional responsibility and authority for the PGS, including the management of the CBSA Security Program.







While certain components of the program rely on expertise residing outside the Comptrollership Branch (Information, Science and Technology Branch [ISTB] and Operations Branch), the overall responsibility and accountability for the Security Program resides with the DSO. Refer to Appendix B for the CBSA Security Program Accountability Structure.

**Program Objectives**
It is essential for the CBSA to have an innovative cost effective and efficient security program in place to address the Agency's responsibilities towards the Canadian public and to ensure that the Agency remains compliant with the spirit, intent and mandated requirements of the PGS and all related directives and standards. The CBSA is also required to adhere with the legal and regulatory requirements applicable to the Agency.

The spirit, intent and mandated requirements of the PGS are summarized by the following policy statements:
- Information, assets, services and employees are safeguarded from compromise and employees are protected against workplace violence;
- Governance structures, mechanisms and resources are in place to ensure effective and efficient management of security at both a departmental and government-wide level;
- Management of security incidents is effectively coordinated within departments and government-wide;
- Interoperability and information exchange are enabled through effective and consistent security and identity management practices; and
- Continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies.

**Definitions for Security Activities**
The management of security can be broken down into the following security program areas:

**Security Administration and Program Coordination** refers to the documentation of policies, standards, guidelines, procedures and baselines regarding internal security requirements and the establishment of appropriate mechanisms associated with agreements involving assets or risks being shared across organizations.

**Security Awareness and Training** involves two components. The focus of Security Awareness is to ensure that all CBSA personnel have been informed of their responsibilities in regard to safeguarding employees, information and assets. On the other hand, Security Training is the provision of technical expertise in order to meet Treasury Board and various regulatory requirements and/or court standards.

**Physical Security** refers to the appropriate physical, technical, procedural and psychological safeguarding of persons and tangible items (assets, facilities, infrastructure, etc.).

**Security Incident Reporting** involves the identification, investigation, reporting, processing and analysis of events associated with security breaches, the loss or damage to assets, of confidentiality, integrity and/or, availability, and relative value or public confidence in the Agency's employees, sensitive assets or operations.







**Information Security (InfoSec)** assures that the appropriate physical, technical, procedural, and psychological safeguards are afforded to information (in all its forms) beginning from the conceptualization of sensitive information through to its final and irrevocable destruction. It should be noted that InfoSec will draw upon the inputs from many other bodies of knowledge, particularly Information Technology Security (ITSec), Physical Security and Personnel Security.

**Communication Security (COMSEC)** involves the application of cryptographic security, transmission and emission security, physical security measures, and operational practices and controls that deny unauthorized access to information derived from telecommunications and that ensure the authenticity of all telecommunications.

**Communications Intelligence Control Officer (COMCO)** is responsible for the management and oversight of classified and sensitive information related to National intelligence interests that has been identified and designated as Special Material. Special Material is all information and material that requires special control for restricted handling under compartmented foreign intelligence systems. Special Material includes (but is not limited to) Signals Intelligence (SIGINT).

**Identity Management** refers to the set of principles, practices, processes and procedures used to realize an organization's mandate and its objectives related to identity.

**Personnel Security** refers to the maintenance of the appropriate standards of conduct, and the review of the reliability and assessment of loyalty to determine the level of security clearance (i.e. reliability, secret and top secret) for all persons given access to the Agency infrastructure (facilities, assets, information, systems, etc.).

**Professional Standards Investigations** involves conducting investigations into on-duty and off-duty suspicions or allegations of employee misconduct relating to the CBSA Code of Conduct, Values and Ethics Code for the Public Service, CBSA policies and violations of criminal and other legislation.

**Information Technology Security (ITSec)** involves the operational, administrative, technical and logical safeguards that are applied to machines or other assets used to communicate information in a variety of forms. ITSec focuses primarily on the application, design, configuration and appropriate use of technology.

**Emergency Management** is the management of emergencies concerning all hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery.

**Business Continuity Planning (BCP)** involves the development and timely execution of plans, measures, procedures and arrangements that ensure minimal or no interruption to the availability of critical services and assets in case of a significant event that disrupts the operations of the Agency. This includes the following:

- Measures aligned with prevention, detection, notification and response to activities under the Business Continuity Planning models; and
- Measures aligned with the prevention / preparation, detection, notification, mitigation and response steps under Emergency Preparedness models.







**IT Continuity Planning** involves the development and timely execution of plans, measures, procedures and arrangements that ensure minimal or no interruption to the availability of critical IT services, systems, data, and infrastructure in case of a disaster that disrupts the operations of the Agency.

**Health and Safety** involves putting in place a program that is in compliance with Part II of the *Canada Labour Code* to ensure that employees are provided with a safe and healthy working environment.

**Security Administration**
The administration of the CBSA Security Program is based on the principles outlined in the PGS, the Directive on Departmental Security Management and the Directive on Identity Management. Each requires the integration of the following concepts within the program:

1. ***Planning***
2. ***Governance***
3. ***Management of Security Risks***
4. ***Monitoring and Oversight***
5. ***Performance Measurement and Evaluation***
6. ***Government-wide support***

## 1. Planning

Departmental security planning, which ultimately results in the identification of the overall security program priorities, revolves around continuous assessment of internal and external risks and their potential impact to the Agency. Historically, many of the security activities have been reactive to Government of Canada and Agency priorities.

Through careful planning, the security organization has evolved and strengthened over time. Significant efforts have been concentrated on performing gap analyses and risk exposures to form the basis for the Departmental Security Plan (DSP). The DSP describes methods for managing security risks and outlines strategies, goals, objectives and timelines for improving the overall security posture of the Agency.

The DSP:
- Provides an integrated view of the Agency's security requirements;
- Identifies security threats, risks and vulnerabilities to determine an appropriate set of control objectives;
- Identifies and establishes additional controls required to meet control objectives and achieve an acceptable level of residual risk;
- Outlines security strategies, objectives, priorities and timelines for improving the Agency's security posture; and
- Defines the processes, roles and responsibilities for evaluating performance, information and progress made.

## 2. Governance







The Security Management Committee (SMC) (Appendix C) has been established as the focal point for consultation and governance in the areas of security, emergency and business continuity management. The SMC is the link between the three branches with functional, business and security roles (ISTB, Operations and Comptrollership) and the branches with an indirect / collateral security role (Programs, Human Resources and Corporate Affairs). SMC membership represents all areas of CBSA (including the Regional Corporate and Program Services Directors) that have a role in the delivery of the security program and is chaired by the DSO.

The SMC members are responsible to ensure the coordination and integration of security activities with departmental operations, plans, priorities and provide advice and support on these areas to:

- The Corporate Management Committee; and
- The Executive Committee (EC).

In addition, bi-monthly security managers' teleconferences to discuss Agency security issues are held. In attendance are the Regional Security Managers and the HQ Security Managers. Occasionally, representatives from other program areas within the Agency are invited to participate.

In addition, the Continuity Operations Security Working Group (COSWG) was established to serve as a consultative body in the areas of corporate security, operations, business continuity and provide advice and updates to SMC during and following significant events.

There are a number of internal and external committees and working groups that are attended by security personnel at various levels to ensure the effective coordination of Agency security program activities within the CBSA and across government.

## 3. Management of Security Risks

Security Risk Management is a systematic approach to assessing threats, analyzing risks and implementing controls. The key steps in the process include the identification, assessment, evaluation and treatment of security risks. As these steps form the very basis for the security program requirements, it is crucial that they become a living cycle.

The Agency is responsible for developing, documenting, implementing and maintaining processes for the systematic management of security risks to ensure continuous adaptation to the changing needs of the department and threat environment.

This is achieved through the integrated approach of multi-disciplinary teams who are responsible for the management of these processes which in turn are implemented by the Headquarters Security Section and Regional Security Offices. The next section will further define the associated program components and how they contribute to the overall management of security risks:

- Security Administration and Program Coordination
- Security Policy, Awareness and Training







- Physical Security
- Information Security (includes Communications Security)
- Information Technology Security
- Identity Management
- Personnel Security Screening
- Professional Integrity
- Professional Standards Investigations
- Headquarters Security and Regional Security
- Emergency Management
- Business Continuity Management
- Information Technology (IT) Continuity Management
- Health and Safety

**Security Administration and Program Coordination**
**Security Policy, Awareness and Training**
The *Security Policy and Program Coordination Section*, in collaboration with the functional authorities, provides the central coordination and governance function required to effectively and efficiently deliver security services and to respond to various requirements stemming from central or lead agencies.

The focus of Security Awareness is to ensure that all CBSA personnel have been informed of their responsibilities in regard to safeguarding employees, information and assets, whereas Security Training is the establishment of the necessary technical knowledge, skills and abilities required to undertake security-related tasks (i.e. deliver the CBSA's Security Program).

Activities include:
- Ensuring that the CBSA security policies, directives, standards, guidelines, and procedures are in compliance with the PGS;
- Developing, implementing, monitoring and reporting on the Departmental Security Plan.
- Coordinating regular communication activities related to HQ/regional security management;
- Reviewing written collaborative arrangements (i.e. MOU, exchange of letters) to ensure that they meet security requirements;
- Coordinating and preparing responses into planning and reporting documents:
  - Management Accountability Framework (MAF)
  - Enterprise Risk Plan (ERP)
  - Internal and external audits
- Coordinating security awareness and training requirements;
- Developing awareness and coordinating training activities and products;
- Maintaining awareness and training records; and
- Delivering security awareness through training and promotion.

**Physical Security**
The Physical Security policy describes the goals, objectives, core activities and responsibilities of the Physical Security program within CBSA.



Physical Security is based upon the theory that the external and internal design of a facility, and specific security controls, can lead to an environment in which the following is accomplished:

- The risk of violence towards employees is reduced;
- The risk of unauthorized access to sensitive assets is reduced; and
- The risk of disruptions to Agency operations is reduced.

This is accomplished by taking certain steps or applying certain measures that are intended to preserve the confidentiality, integrity, availability and value of CBSA assets. These steps are referred to as security controls and are generally organized in terms of administrative controls (such as policies, standards, procedures, etc.), physical controls (barriers, lighting, alarms, closed-circuit video equipment, containers, etc.), procedural controls (requirements for two-person integrity checks, logging of access) and technical controls (design practices). These controls are organized into what are referred to as protective systems.

**Information Security**

One of the overarching principles of the PGS is that information is protected against compromise whether accidental or deliberate. Information is crucial to the delivery of operations and therefore its confidentiality, integrity and availability is of utmost importance.

The *Information Security Section* is responsible for the implementation of security processes related to the protection of the Agency's information regardless of format (hard copy vs. electronic) and to a degree the systems (hardware and software) supporting it. It should be noted that Information Security (InfoSec) will draw upon the inputs from many other bodies of knowledge, particularly Information Technology Security (ITSec), Physical Security and Personnel Security.

Activities include:

- Program monitoring and oversight through the provision of assistance and guidance to CBSA stakeholders related to Information Security and monitor the effectiveness of the security controls.
- Risk management through the development, documentation, implementation and maintenance of processes for the systematic management of information security risks.
- Assisting in maintaining the integrity of all CBSA information holdings and security of these systems;
- Participating in the Security Assessment and Authorizations (SA&A) of Information Systems which supports risk management practices by reviewing Threat and Risk Assessments (and other documents) to properly identify risks to the confidentiality, integrity and availability of information assets;
- Managing Communications Security (COMSEC) asset administration, distribution and support;
- Managing and providing oversight of classified and sensitive information related to national intelligence interests – Communications Intelligence Control (COMCO);
- Providing Integrity Monitoring by:
  - coordinating network and database monitoring activities (e.g. e-mail, web usage, systems storage)







  - providing IT investigations and network monitoring support for Professional Standards Investigations;
  - Coordinating and approving web access requests and monitor web use;
- Participating as member of the release authority for information to third party applicants (e.g. database extractions, employee e-mail and/or files); and
- Performing database security audits (e.g. CPIC).

**Information Technology Security**
The Information Technology (IT) Security Program is a subcomponent of the Agency Security Program and is managed by the IT Security and Continuity Division (ITSCD) of the Information, Science, and Technology Branch (ISTB). Although ISTB has functional responsibility for security activities identified in the following section, all planning, policies and efforts are coordinated and aligned with the overall Agency Security Program led by the DSO.

An IT Security Coordinator (ITSC) is responsible for maintaining a functional reporting relationship with the DSO. IT Security roles are specified both throughout this framework and in the Agency Security Volume. SPSD and ITSC developed a comprehensive IT Security Program Governance Arrangement that establishes the Governance Framework for the delivery of IT Security Services.

The IT Security Program, based on the IT Security Program Charter, is structured to support IT Security service delivery in these major areas:

The *Risk Assessment and Consultation (RAC) section* works with CBSA clients to ensure Agency applications and systems are developed and implemented with approved and appropriate levels of IT security controls that ensure CBSA's systems, information and data is protected from unauthorized disclosure, misuse or access.

The RAC uses assessment tools to analyze and determine if there are IT security requirements. The goal is to be a service enabler that supports the business of the Agency.

The RAC assesses IT security risks against CBSA IT systems, applications and data, and provides guidance and recommendations that would allow the risks to be mitigated to an acceptable level.

Activities include:
- Aligning with the CBSA's vision and mission to provide optimal, reliable service delivery for integrated border services that support national security and public safety priorities; and
- Protecting CBSA information and data from compromised or unauthorized access consistent with Agency policies and the Policy on Government Security (PGS).

The IT Security *Cyber Protection Centre (CPC) section* is responsible for establishing and maintaining consistent IT security management, services and projects. The CPC follows the guidance provided by the key government organizations, including the Treasury Board Secretariat Operational Security Standard on the Management of Information Technology Security (MITS).

The CPC ensures that the CBSA has the processes and procedures in place to respond and react in a timely manner to cyber events and incidents that may negatively impact IT assets.







The CPC is responsible for monitoring and responding to cyber alerts provided by the Canadian Cyber Incident Response Centre. This includes coordination with security partners such as Communication Security Establishment Canada (CSEC), Shared Services Canada (SSC), Canada Revenue Agency (CRA), and the Royal Canadian Mounted Police (RCMP) to:

- Contain and mitigate possible threats;
- Respond to cyber incidents and address them in a timely manner; and
- Provide updates to management to keep them apprised of the situation and to find a solution to mitigate the level of risk.

The CPC provides technical services that comprise of evaluations and recommendations for security solutions, for example researching secure solutions for the use of iPads within the CBSA, which can include product evaluations and testing. The CPC also provides Vulnerability Assessment (VA) services for systems and applications.

The *Governance and Strategy (G&S) section* has a strategic focus that complements the IT Security operational aspects undertaken by other sections within the ITSCD.

The G&S provides strategic planning and reporting for the CBSA IT Security Program, as well as providing key contributions with the development of Agency IT Security policy / standards and training / awareness programs.

Activities include:
- Providing advice and guidance for inquiries related to IT Security policy interpretation; and
- Providing, upon request, customized IT Security awareness sessions to complement the mandatory online awareness modules.

The G&S maintains liaison with CBSA business stakeholders to ensure continuous alignment of IT Security strategic programs with Agency business requirements. The section also closely liaises with the Security and Professional Standards Directorate of the Comptrollership Branch.

**Identity Management**
Identity Management is an identifiable and integral element of departmental programs, services and activities. It is at the heart of public administration and most of the Agency's business processes. Once an identity is established, all subsequent government activities, ranging from safeguarding of assets to delivering services, entitlements, and responding to emergencies rely upon this identity.

There is a clear need for a consistent approach to identity management. This will ensure that security requirements are met and that services are developed, administered and delivered to the right clients. The development and implementation of this standardized approach will also permit a robust, scalable and flexible solution for the proper validation of identity information.

*Managers at all levels are responsible for:*
- Ensuring there is a rightful need for identification and the lawful authority to identify for a specific program or in support of law enforcement, national security or defence activities;
- Reporting identity management risks (e.g. change of circumstances, errors, malfeasance, etc.), program impacts, required levels of assurance and risk mitigation options;







- Selecting an appropriate set of identity data (such as personal attributes or identifiers) to sufficiently distinguish a unique identity to meet program needs, which is proportionate to identified risks and flexible enough to allow for alternative methods of identification, when appropriate; and
- Implementing identity information sharing solutions that adhere to common Government of Canada standards.

*Human Resources Managers are responsible for*:
- Ensuring each CBSA employee (indeterminate, term, casual, part-time, students, contractors, consultants and temporary agency personnel including those deployed, seconded or assigned) is assigned a unique personal record identifier (PRI) for the management of employee-related information and transactions; and
- Ensuring each employee who must be identified to one or more remittance agencies outside the federal public service is assigned an Individual Agency Number (IAN).

**Personnel Security Screening**
All individuals considered for employment with the Agency are subject to personnel security screening to obtain a Reliability Status, and, if required by the position, a Security Clearance prior to being appointed to a position. This process is supported by the *Personnel Security Screening Section.*

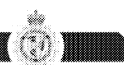
Activities include:
- Overseeing the conduct of all personnel security screening activities;
- Overseeing reviews for cause and revocations when adverse information places an individual's clearance at risk;
- Making recommendations to the Departmental Security Officer (DSO) on the issuance of clearances;
- Maintaining personnel security screening files for all CBSA employees;
- Leading the conduct of reliability assessments – verifying trustworthiness, honesty, integrity and reliability, which includes conducting credit and criminal history checks, and other enhanced checks such as integrity interviews;
- Coordinating the Canadian Security Intelligence Service (CSIS) assessments as they relate to an individual's loyalty to Canada for Secret and Top Secret clearance requests; and
- Providing policy and functional guidance to Regional Security Practitioners.

**Professional Integrity Program**
The Professional Integrity Program (PIP) was established to ensure a culture of professional integrity among its employees and a concerted approach to the management of professional integrity related risks. For the CBSA, professional integrity means that its employees are responsible for:

- Exercising their authority in an honest, open and fair manner;
- Accepting responsibility for their actions in order to build and maintain a reputation of trustworthiness and accountability;
- Treating others in a respectful manner;
- Doing what is right even when nobody is looking; and
- Safeguarding the physical and informational assets of the CBSA.







Activities include:

- Raising awareness of professional integrity across the CBSA;
- Clearly communicating and reinforcing the expected standards of professional conduct, both on- and off-duty, to all CBSA employees;
- Ensuring that CBSA employees know how to detect, report, avoid and mitigate situations involving misconduct; and
- Conducting oversight activities to ensure that professional integrity risks are identified, reported, continually monitored and mitigated.

**Professional Standards Investigations**

All organizations establish standards of behavior and conduct that they expect their employees to demonstrate and abide by. At the CBSA, these are outlined in our Code of Conduct which is an extension of the Values and Ethics Code for the Public Service amongst other policy instruments.

The Codes advise employees that they are expected to conduct themselves both on and off-duty in a manner that is beyond reproach and in keeping with government policies and procedures. Transgressions that are contrary to these expectations may be considered misconduct.

Misconduct includes any action or inaction on or off duty whereby an employee contravenes an act (including the Criminal Code of Canada), a regulation, a rule, a CBSA policy, an approved procedure, or the CBSA Code of Conduct, or participates in an activity which brings the CBSA into disrepute or affects the CBSA's relationship with other law enforcement organizations.

When adverse information concerning a CBSA employee is discovered by or disclosed to the PSPSD, the *Security and Professional Standards Analysis Section* of PSPSD is responsible for:

- Conducting preliminary assessments of disclosures to determine the probability that the alleged wrongdoing/misconduct has, is or will occur, the seriousness of the alleged wrongdoing/misconduct and whether an administrative investigation (i.e. Review for Cause, Fact Finding, Professional Standards Investigation) is warranted;
- Providing guidance and support, and tracking the status of local management fact findings, reviewing preliminary assessment reports conducted by local management and assessing findings;
- Tracking disclosure files and reporting on the status including preliminary assessments, rejections, referrals made and investigations in progress;
- Administering and maintaining a database with pertinent reporting data from all disclosures, investigations, findings and resultant actions;
- Providing up-to-date statistics on disclosures, investigations, findings and resultant actions for analysis, planning and performance measurement purposes; and
- Providing annual and semi-annual briefings of misconduct investigation trends and patterns to the Executive Committee.

To this end, the *Professional Standards Investigations Section* is responsible for:

- Providing centralized and independent administrative investigation services on behalf of CBSA senior management;
- Conducting investigations into allegations of on and off-duty employee misconduct, such as violations of the CBSA Code of Conduct, the Values and Ethics Code for the Public Service and other government policies;







- Preparing reports on findings and conclusions in relation to suspected misconduct;
- reporting to and liaising with law enforcement agencies regarding suspected criminal offences involving CBSA employees;
- Providing testimony in administrative tribunals and court proceedings; and
- Providing observations to senior management when deficiencies or weaknesses in policy or procedures are identified, as the result of an investigation.

**Headquarters Security and Regional Security Offices - Program Delivery**
The *Headquarters Security Section* and the *Regional Security Offices* are responsible for providing advice and guidance to Headquarters and Regional staff and to ensure that the physical security posture of the space occupied by CBSA is adequate to safeguard Agency employees, information and assets.

Activities include:
- Providing advice, guidance and training to management and employees on all security matters;
- Providing training, advice and guidance relating to building evacuation plans and teams;
- Ensuring measures are in place for the protection of employees where occupations, demonstrations, bomb threats, fire or acts of violence may occur (i.e. up-to-date emergency evacuation plans);
- Conducting security inspections/reviews of new or existing facilities to assess security posture, identify vulnerabilities and provide security recommendations/specifications and once recommendations have been implemented sign-off on the facility;
- Providing centralized services and ensures the proper control and safeguarding of all controlled assets (COMSEC Equipment, badges, firearms and ID/Access Cards).;
- Performing audit and monitoring functions in regard to controlled assets (i.e. Arming Rooms);
- Coordinating  all requests for Personnel Security Screening submissions;
- Conducting Threat and Risk Assessments, site reviews and security sweeps;
- Coordinating the testing, servicing, monitoring of electronic access control and intrusion alarm systems;
- Ensuring that the national physical security program is implemented and adhered to;
- Ensuring that security requirements are included in all contracts, providing advice and guidance, and acting as the approval authority for Security Requirement Check List sign-off as delegated by the DSO;
- Administering a security incident reporting network, conduct investigations and report on security incidents/breaches/violations and recommend corrective measures to management;
- Providing silent hour Duty Officer service and respond to calls (intrusion alarms, guard enquiries regarding access, employee assistance, etc.);
- Updating the Employee Notice Line in case of emergencies with respect to facility disruptions or closures;
- Maintaining an inventory of all combination locks and ensure that cabinets and locks are tagged, inventoried and requests for combination changes are conducted; and
- Participating and representing Security on committees as required (e.g. Building Emergency Organization, Occupational Health & Safety).

**Emergency Management**







**Comptrollership Branch**
Emergency Management (EM) is the management of emergencies concerning all hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery.

Activities include:
- Providing strategic program oversight of the CBSA Comprehensive Emergency Management Program (includes Security, Emergency Management (Operations Branch), BOC, IT, BCM, HR, Communications and Legal);
- Leading and coordinating the development of comprehensive emergency management frameworks;
- Developing, implementing, and maintaining the CBSA Strategic Emergency Management Plan (SEMP) as well as its Emergency Management Risk Register;
- Providing oversight, input and monitoring of a comprehensive CBSA exercise calendar, which integrates operational readiness, business continuity planning and IT continuity exercises; and
- Managing and updating the Agency Employee Notice Line (ENL) for the National Capital Region (NCR).

**Operations Branch, National Border Operations Centre (NBOC)**
The *Emergency Management Section* provides program oversight and direction for operational Emergency Management measures in the field and maintains Operational Readiness, and coordinates with relevant Government of Canada partners such as the Government Operations Centre, Public Safety Canada and other stakeholders on interdepartmental security initiatives such as the Federal Emergency Response Plan (FERP), the Maritime Emergency Response Protocol (MERP), and others.

Activities include:
- Providing program management with respect to operational emergency management measures and assisting Regions in setting up and maintaining emergency management plans, port of entry business continuity planning and plans, Regional Operations Centre (ROC) plans, regional critical incident management plans, Incident Command System (ICS) training, and other EM plans and products;
- Promoting and coordinating Operational Readiness within the Regions as well as coordinating the Regional Emergency Management coordinators' network;
- Ensuring full integration of Operational EM activities into the Comprehensive Emergency Management Framework; and
- Leading on operational, regional/POE BCP and other exercises.

**Business Continuity Management**
Business Continuity Management (BCM) involves the development and timely execution of Business Continuity Plans (BCP), related activities, procedures and arrangements that ensure minimal or no interruption to the availability of critical services and assets to the Canadian Public in case of a significant event that disrupts the operations of the Agency.

Activities include:



- Leading the implementation of the Business Continuity Process within the Emergency Management framework and ensure Business Continuity Plans are in place for all identified critical services and critical support services;
- Leading Business Impact Analysis (BIA) to assess the impact of events on the Agency's services, assets and dependencies;
- Coordinating plan readiness through exercising;
- Providing strategic monitoring and oversight; and
- Liaising and integrating with central agencies and Other Government Departments business continuity initiatives and requirements.

**Information Technology (IT) Continuity Management**
IT Continuity Planning involves the development and timely execution of plans, measures, procedures and arrangements that ensure minimal or no interruption to the availability of critical IT services, systems, data, and infrastructure in case of a disaster that disrupts the Agency's operations.

Activities include:
- Developing and maintaining the IT continuity program;
- Developing and maintaining the disaster recovery program;
- Administering and supporting the Planning, Response, Recovery, Emergency Preparedness (PRREP) software;
- Developing and implementing IT continuity awareness programs;
- Developing and implementing programs and operational activities for effective response and management of disasters affecting information technology, including coordination with external agencies as required;
- Leading on disaster recovery exercises;
- Monitoring and reporting on situations that impact on CBSA IT operations;
- Providing the CBSA focal point for 24/7 IT disaster response through the IT Response Centre (ITRC);
- Providing ongoing evaluation of the recovery capabilities managed by external service providers to ensure all CBSA requirements are being met;
- Developing, maintaining, and monitoring IT continuity strategies, policies, processes and risk management frameworks while ensuring compliance to MITS and Government of Canada security policies, directives and standards; and
- Leading the implementation of the IT Continuity Program within the Emergency Management framework and ensure IT Continuity and Disaster Recovery Plans are in place for all critical IT services and Systems.

**Response Situational Awareness and Coordination**
**Border Operations Centre (BOC)**
The Border Operations Centre (BOC) operates a 24/7 centralized communications and coordination hub for reporting events and issues which affect the CBSA. The BOC contributes to a consistent national response and provides an established process for notification and management significant events and emergencies. The BOC provides operational support to employees in the field both in Canada and abroad.



Activities include:

- Identifies and ensures senior management awareness of pending events, activities, and issues that may impact the fulfillment of Agency mandate and/or the public perception of the Agency;
- Central point of contact for stakeholders (internal and external),and offices of primary interest to address significant events;
- Support/backup to Agency business continuity planning (BCP); and
- Supports Agency management/response through consistent communication/reporting of events, issues and incidents which impact the Agency.

**Health and Safety**

The CBSA is responsible for ensuring the health and safety of its employees and visitors to its facilities. In the context of the CBSA Security Program, this relates directly to protecting employees against workplace violence and other requirements set forward by the *Canada Labour Code* Part II and other TBS Policy Instruments. Although the accountability to ensure employee safety within the security context rests with the DSO, the *Health and Safety Division* of the Human Resources Branch / Labour Relations and Compensation Directorate is responsible for ensuring that there is a program in place to protect the health and safety of employees at the work place.

Activities include:

- Providing advice and guidance to CBSA Management on issues and compliance related to the *Canada Labour Code* Part II, TBS National Joint Council Directives;
- Developing and ensuring that the 'Violence Prevention in the Workplace' policy is reviewed on a regular basis;
- Developing a mandatory health and safety program for all employees and monitor that all employees receive appropriate training on that program;
- Acting as the Secretariat for the Policy Health and Safety Committee;
- Providing coordination with SPSD on matters relating to protection of employees against workplace violence; and
- Liaising with SPSD regarding emergency procedures and evacuation plans requirements.

## 4. Monitoring and Oversight

Monitoring and oversight is required in order to track progress and communicate results. *Program Monitoring and Risk Evaluation* ensures that: the Agency security program consistency is supported by improved performance monitoring and reporting through quarterly reporting to EC; and that the delivery of security services is more fully aligned to Agency priorities and operational requirements. Activities include: Agency Performance Reporting (APR); Functional Management Model (FMM) coordination and reporting; Performance Measurement Planning (PMP) and Reporting.

Activities include:

- Establishing and maintaining a monitoring program to support the functional reporting relationship with the Regional Directors of Security, Regional Security Managers and HQ Security Program Personnel;
- Coordinating reporting for Performance Measurement activities;
- Developing a comprehensive trends database to monitor, analyze and interpret trends;





- Developing and providing oversight of a monitoring strategy related to key security controls and associated metrics; and
- Coordinating performance measurement standards for the Security and Professional Standards Directorate programs.

## 5. Performance Measurement and Evaluation

Quarterly reviews are conducted to assess whether the Agency Security Program is effective, whether the goals, strategic objectives and control objectives detailed in the CBSA Departmental Security Plan (DSP) were achieved and whether the plan remains appropriate to the needs of the Agency and the government as a whole.

On an ongoing basis, performance is measured to ensure that:

- A quality assurance program exists to verify that security controls meet Agency security requirements in the most efficient and effective manner; and,
- An acceptable level of residual risk is achieved and maintained.

The CBSA is responsible for reporting periodically to TBS via the Management Accountability Framework (MAF) on the status and progress of implementation of the PGS and on the results of ongoing performance measurement.

## 6. Government-wide support

The CBSA provides leadership, demonstrates innovation and contributes to the government-wide security program on an on-going basis by participating in:

- The ADM and DG Security Committees chaired by TBS;
- Various central agency led working groups; and
- The ITSC / DSO inter-departmental community meetings chaired by TBS as well as the Cyber Security Working group.



# Appendix B – CBSA Security Program Accountability Structure

CBSA Security Program Accountability Structure

- **President / Executive Vice-President CBSA**
  - Vice-President Comptrollership Branch (connected to President / Executive Vice-President CBSA)
    - Director General / Departmental Security Officer (direct reporting to Vice-President Comptrollership Branch; indirect reporting to President / Executive Vice-President CBSA)
      - Security and Professional Standards Directorate
        - Director Security and Professional Integrity Programs Division
          - Manager Security Policy and Program Coordination
          - Manager Program Monitoring & Risk Evaluation / Professional Integrity Program
          - Manager Headquarters (HQ) Security
        - Director Personnel Security and Professional Standards Division
          - Manager Professional Standards Investigations
          - Manager Security & Professional Standards Analysis
          - Manager Personnel Security Screening
        - Director Infrastructure and Information Security Division
          - Manager Physical Security
          - Manager Information Security
  - Vice-President Operations Branch (indirect reporting to Director General / Departmental Security Officer)
    - Regions
      - Directors, Corporate and Program Services Division Regional Security Managers (indirect reporting to Director General / Departmental Security Officer)
  - Vice-President Information, Science and Technology Branch (indirect reporting to Director General / Departmental Security Officer)
  - Vice-President Programs Branch
  - Vice-President Human Resources Branch
  - Vice-President Corporate Affairs Branch
  - Senior General Counsel Legal Services

Legend:
- ·········· Indirect reporting
- ——— direct reporting

# Appendix B – CBSA Security Program Accountability Structure

The above flowchart depicts the Canada Border Services Agency Security Program Accountability Structure.

The Physical Security Manager and the Information Security Manager report directly to the Director of Infrastructure and Information Security Division.

The Personnel Security Screening Manager, the Security & Professional Standards Analysis Manager and the Professional Standards Investigations Manager report directly to the Director of the Personnel Security and Professional Standards Division.

The Headquarters (HQ) Security Manager, the Program Monitoring & Risk Evaluation / Professional Integrity Program Manager and the Security Policy and Programs Coordination Manager report directly to the Director of Security and Professional Integrity Programs Division.

The Director of Infrastructure and Information Security Division, the Director of the Personnel Security and Professional Standards Division and the Director of Security and Professional Integrity Programs Division all report directly to the Director General / Departmental Security Officer of the Security and Professional Standards Directorate.

The Director General / Departmental Security Officer reports directly to the Vice-President of the Comptrollership Branch and reports indirectly to the President / Executive Vice-President of the Canada Border Services Agency.

The Vice-President of the Comptrollership Branch reports directly to the President / Executive Vice-President of Canada Border Services Agency.

The Directors, Corporate and Program Services Division as well as the Regional Security Managers in the regions report directly to the Vice-President of the Operations Branch.

The Directors, Corporate and Program Services Division as well as Regional Security Managers in the regions report indirectly to the Director General / Departmental Security Officer.

The Senior General Counsel of Legal Services, the Vice-President of the Corporate Affairs Branch, the Vice-President of the Human Resources Branch, the Vice-President of the Programs Branch, the Vice-President of the Information, Science and Technology Branch and the Vice-President of the

Operations Branch all report directly to the President / Executive Vice-President of Canada Border Services Agency.

The Vice-President of the Information, Science and Technology Branch and the Vice-President of the Operations Branch report indirectly to the Director General / Departmental Security Officer and the President / Executive Vice-President of CBSA.






**Appendix C – Security Management Committee Terms of Reference**

# Security Management Committee

## Terms of Reference

1. **Position in Governance Structure**

The Security Management Committee (SMC) is a senior management level committee chaired by the Departmental Security Officer (DSO). It provides advice and guidance relating to the strategic management of the Agency Security Program to the Corporate Management Committee (CMC) and to the Executive Committee, as required.

2. **Mandate**

The mandate of the SMC is to:

- set strategic direction for CBSA corporate security;
- serve as a consultative body for emerging and ongoing security issues;
- establish strategic direction and provide functional guidance and support in this area to the V.P., Comptrollership;
- bring forward contentious issues to the Corporate Management Committee (CMC) for further deliberation and decision (p. ex. security related impacts relevant to program/policy development);
- bring forward to the Executive Committee (EC) and or the President, security issues that solely remain under the President's responsibility as per the Delegation of Authority to the Departmental Security Officer (DSO) and the Policy on Government Security.

3. **Membership**

The membership is composed of inter-branch and regional representation:

Chairperson







- Departmental Security Officer (DSO) and Director General, Security and Professional Standards Directorate, Comptrollership Branch

Alternate Chairperson

- Director General, National Border Operations Centre, Operations Branch

Members

- Director General, Enterprise Services Directorate, Information, Science and Technology Branch
- Director General, Strategic Risk and Modernization Directorate, Programs Branch
- Director General, Labour Relations and Compensation Directorate, Human Resources Branch
- Director General, Infrastructure and Environmental Operations Directorate, Comptrollership Branch
- Senior Director, Communication Advisory Services Division, Corporate Affairs Branch
- Director, Security and Professional Integrity Programs Division, Comptrollership Branch
- Director, Personnel Security and Professional Standards Division, Comptrollership Branch
- Director, Infrastructure and Information Security Division, Comptrollership Branch
- Manager, Emergency Management Section, Operations Branch
- Director, IT Security and Continuity Division, Information, Science and Technology Branch
- Regional Director General (Atlantic Region)
- Regional Director, Corporate and Program Services Division, responsible for Security (Atlantic Region)
- Regional Director General (Quebec Region)
- Regional Director, Corporate and Program Services Division, responsible for Security (Quebec Region)
- Regional Director General (Northern Ontario Region)
- Regional Director, Corporate and Program Services Division, responsible for Security (Northern Ontario Region)
- Regional Director General (Greater Toronto Area Region)







- Regional Director, Corporate and Program Services Division, responsible for Security (Greater Toronto Area Region)
- Regional Director General (Southern Ontario Region)
- Regional Director, Corporate and Program Services Division, responsible for Security (Southern Ontario Region)
- Regional Director General (Prairie Region)
- Regional Director, Corporate and Program Services Division, responsible for Security (Prairie Region)
- Regional Director General (Pacific Region)
- Regional Director, Corporate and Program Services Division, responsible for Security (Pacific Region)

**Subject Matter Experts (SMEs) may be invited as guests for specific agenda items as required at the discretion of the Chairperson.

Secretariat

Secretariat support will be provided by:

- Senior Security Advisor, Security Policy and Program Coordination Section, Comptrollership Branch

The Secretariat is responsible to:

- send invitations to all members to contribute agenda items three (3) weeks prior to each meeting;
- draft agendas (current and forward) and obtain approval from the Chairperson;
- provide final agendas and meeting material to all members four (4) days prior to each meeting;
- prepare the Records of Decisions and Key Action Items after each meeting for the Chairperson's review and approval prior to sending them to all the members for their review and comments within four (4) days after the meeting is held;
- follow up on key action items as required and report to the Chairperson.

## 4. Proxies to Meetings

Members of SMT shall nominate one (1) permanent pre-determined Director-level proxy to attend meetings where the member cannot attend.

## 5. Quorum Requirement







A minimum of eight (8) members in addition to the Chair or Alternate Chair are required for the meeting to be recognized as an authorized meeting, unless otherwise specified by the Chairperson.

If the Chairperson is not available to attend, the Alternate Chairperson will preside the meeting.

## 6. Authority

The Chairperson of the SMC has the authority to:

- set the overall strategic direction of the committee;
- set the annual strategic direction of the Committee;
- approve agendas and request items be brought forward at a specified date;
- decide on items put before the Committee while seeking to build consensus among members in carrying out this duty;

The Committee may strike subcommittees, chaired by standing committee members, which could include others to assist in the delivery of the Committee's mandate.

## 7. Duties and Responsibilities

The duties and responsibilities of the SMC include:

Security

The SMC will ensure the protection and safety of employees, the confidentiality, integrity and availability of all CBSA assets, including information, and ensure the delivery of core CBSA security-related programs by:

- providing advice and direction on issues related to all elements of security: personnel, information, physical, controlled assets and information technology;
- ensuring appropriate linkages and consultation occurs with affected stakeholders on security issues;
- ensuring that security awareness programs are developed for managers and staff on their roles and responsibilities related to security;
- ensuring that security policies, procedures, standards, and program delivery guidelines are updated in response to changes (i.e. Treasury Board Secretariat requirements, lessons learned, etc.) and communicated to CBSA employees;
- providing direction and endorsement of security policies (including policy instruments such as directives, standards and







their appendices that may have significant impact on programs), programs and priorities;

- reviewing and endorsing security activities in relation to the strategic plan for security activities;
- reviewing performance management activities as well as key security program activities;
- reviewing and approving security program;
- developing sub-committees to address specific issues as required;
- ensuring that a security-related monitoring and reporting program is in place and that reports to senior management are provided on an ongoing basis; and,
- collaborating and resolving issues impacting in the domains of security, emergency management and business continuity reported by the Continuity Operations Security Working Group (COSWG), during SMC meetings.

**8. Frequency and Duration**

The SMC shall meet every two (2) month for a period of two (2) hours and will alternate with the COSWG which will also be held every two (2) months.

The rescheduling of committee meetings will be carried out on an "exception-only" basis.

The Chairperson shall convene ad hoc meetings as required.

**9. Performance Management**

The Chairperson of the SMC shall review the progress of the committee against the strategic plan on a quarterly basis. This will ensure that the work of the Committee is appropriately aligned to, and supports the achievement of the Agency's strategic objectives.

Revised May 12th, 2014





Agence des services frontaliers du Canada | Canada Border Services Agency



# Cadre de gestion du programme de sécurité de l'ASFC

PROTECTION • SERVICE • INTÉGRITÉ

Canada



# Table des matières

Agence des services frontaliers du Canada | Canada Border Services Agency



# Cadre de gestion du programme de sécurité

## 1. Objet

Le présent cadre vise à définir toutes les exigences du programme en vertu de la *Politique sur la sécurité du gouvernement* (PSG) qui ont une incidence sur l'Agence des services frontaliers du Canada (ASFC), et à préciser l'ensemble des obligations de rendre compte, des rôles et des responsabilités se rapportant au programme de sécurité de l'ASFC, en plus de fournir une orientation sur la structure relative à la gestion et à la gouvernance de la sécurité à l'échelle de l'Agence. Ainsi, les employés et les gestionnaires de tous les échelons à l'ASFC seront à même de gérer les risques pour la sécurité et de protéger l'information, les biens, les services et les personnes avec efficacité, afin de veiller à la continuité des services et des opérations pour le public canadien, tout en imposant un faible niveau de risque aux autres ministères et au gouvernement dans son ensemble. Cette notion traduit les principes de la gouvernance efficace, de la gestion, de la planification, du contrôle et de l'évaluation des risques, et de l'amélioration continue.

Ce cadre offre une direction et une orientation stratégiques quant à la conception, à l'élaboration et à la mise en œuvre du programme de sécurité de l'ASFC et de ses sous-programmes. Il établit les paramètres de gouvernance requis par les lois et les politiques.

Ce cadre est appuyé par des directives, des normes, des lignes directrices et des procédures qui fournissent des précisions sur le sujet. Veuillez consulter le Volume de sécurité de l'ASFC pour obtenir de plus amples renseignements.

## 2. Date d'entrée en vigueur

La date d'entrée en vigueur du Cadre de gestion du programme de sécurité de l'Agence des services frontaliers du Canada (ASFC) est le 23 janvier 2015.

## 3. Application

Ce cadre et les documents connexes s'appliquent à l'ensemble de l'Agence, ce qui comprend :

- la totalité des propriétés, des installations et des biens (y compris l'information);
- tous les employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), les contractuels et les employés des agences privées ainsi que les personnes en détachement ou affectées à l'Agence (dont les étudiants);
- les visiteurs, les bénévoles et toute personne se trouvant physiquement à l'intérieur ou à l'extérieur d'une installation de l'ASFC, ou dans une zone contrôlée par celle-ci.







## 4. Contexte

La sécurité du gouvernement est une garantie de protection des employés et des biens contre tout préjudice. La mesure avec laquelle le gouvernement veille à sa propre sécurité a une incidence directe sur sa capacité de protéger ses biens clés et sur la prestation continue de services qui contribue à la santé, à la sûreté, au bien-être économique et à la sécurité de tous les Canadiens.

La sécurité dans le secteur public et la confiance des Canadiens dans les capacités de leur gouvernement à les protéger eux, leurs possessions et leur identité, sont directement reliées. Tous les jours, le gouvernement du Canada interagit directement avec les Canadiens pour leur offrir les services auxquels ils ont droit. Pour le faire avec efficacité, le gouvernement doit bien établir l'identité des personnes et des institutions avec lesquelles il traite. Cela donne lieu au stockage et à la manipulation de vastes quantités d'informations personnelles et d'informations gouvernementales, qui doivent demeurer confidentielles en tout temps et auxquelles on accède seulement en fonction du besoin de savoir. Les fonctionnaires qui ont accès à des renseignements, à des biens et à des services du gouvernement doivent être dignes de confiance, fiables et loyaux. De ce fait, un large éventail d'activités gouvernementales, qui vont de la protection de l'information et des biens à la fourniture de services, d'avantages sociaux et de prestations, en passant par les interventions en cas d'incidents ou d'urgence, repose sur cette confiance.

À l'ASFC, la gestion de la sécurité est un processus vivant et dynamique qui doit faire l'objet d'une évaluation constante et d'une gestion proactive des menaces internes et externes et des risques qui y sont associés. Cela comprend la mise en œuvre, la surveillance et le maintien de contrôles de gestion interne adéquats, notamment la prévention (atténuation), la détection, l'intervention et la reprise des activités. La gestion de la sécurité est en lien direct avec d'autres fonctions de gestion, dont l'accès à l'information et la protection des renseignements personnels, la gestion des risques, la gestion des urgences et de la continuité des activités, les ressources humaines, la santé et la sécurité au travail, l'immobilier, la gestion du matériel, la gestion de l'information, la technologie de l'information et les finances. La gestion de la sécurité suit et respecte les règles de justice naturelle et les principes d'équité procédurale afin de garantir la protection des droits des personnes. À l'ASFC, la sécurité est à son mieux lorsqu'elle est intégrée à la culture et aux opérations au quotidien. Il s'agit du seul moyen de garantir que le programme de sécurité aura une incidence favorable sur les employés et la direction.

## 5. Autorité

Le présent cadre est fondé sur l'article 7 de la *Loi sur la gestion des finances publiques*, sur la *Politique sur la sécurité du gouvernement (PSG)* du Secrétariat du Conseil du Trésor (SCT), et sur la *Directive sur la gestion de la sécurité ministérielle*.

Ce document doit être lu conjointement avec les directives, normes, lignes directrices et procédures connexes en matière de sécurité de l'ASFC présentées dans le Volume de sécurité de l'ASFC et dans les bulletins et avis de sécurité périodiques publiés par l'agent de sécurité du ministère (ASM). Il







invitera le lecteur à consulter des ressources supplémentaires, au besoin. Le présent cadre, ainsi que les autres instruments de politique, se trouvent dans le Volume de sécurité de l'ASFC.

## 6. Objectif

Le présent cadre vise à établir des principes en particulier, à mettre au point une approche intégrée pour la gestion du programme de sécurité de l'ASFC, et à cerner toutes les exigences du programme de sécurité dans le cadre de la *Politique sur la sécurité du gouvernement* (PSG) ayant une incidence sur l'ASFC. Ainsi, l'Agence fera l'objet d'une gestion efficiente, efficace et responsable en matière de sécurité.

## 7. Résultats escomptés

L'ASFC se doit de mettre en œuvre un programme de sécurité rentable et efficient pour s'acquitter de ses responsabilités à l'égard de la population canadienne, et pour se conformer à l'esprit, à l'intention et aux exigences de la *Politique sur la sécurité du gouvernement (PSG), de la Directive sur la gestion de la sécurité ministérielle*, ainsi que de la *Directive sur la gestion de l'identité* et aux normes connexes.

Parmi les résultats escomptés du présent cadre, notons :

- l'information, les biens et les services ne sont pas compromis et les employés sont protégés contre la violence en milieu de travail;
- la définition claire des obligations de rendre compte et des rôles et responsabilités en matière de sécurité à l'échelle de l'Agence, tant sur le plan individuel que sur le plan organisationnel;
- l'établissement et le maintien d'une culture de sécurité au sein de l'Agence;
- l'harmonisation de la stratégie, des processus et des ressources en vue de maintenir une posture de sécurité efficace et efficiente partout à l'ASFC;
- l'uniformité des pratiques de gestion de la sécurité et l'appui à l'interopérabilité et à l'échange d'information, dans un environnement sûr et efficient sur le plan économique;
- la surveillance active des changements apportés à l'environnement et la production de rapports connexes, afin de pouvoir intervenir rapidement dans le cadre de menaces, de vulnérabilités et d'incidents nouveaux et existants;
- la poursuite des opérations et des services gouvernementaux en cas d'incidents relatifs à la sécurité, d'interruptions ou d'urgences;
- la gestion efficace de la sécurité pour garantir que l'ASFC n'augmente pas indûment les risques pour elle-même, les autres ministères et le gouvernement dans son ensemble;
- les structures de gouvernance, les mécanismes et les ressources sont en place pour assurer la gestion efficace et efficiente de la sécurité, tant au sein de l'Agence que dans l'ensemble du gouvernement.







# 8. Rôles et responsabilités généraux

Comme le précisent les sections qui suivent, la haute direction, l'ASM, les gestionnaires de tous les échelons et les employés de l'ASFC sont responsables de la mise en œuvre des contrôles de sécurité et de la réalisation des objectifs s'y rattachant.

## Président

Le président est responsable globalement de la mise en œuvre et de la gouvernance efficaces de la gestion de la sécurité et de l'identité à l'Agence, en plus de partager la responsabilité à l'égard de la sécurité du gouvernement dans son ensemble. Plus précisément, il incombe au président de :

- protéger les employés et les biens de l'ASFC;
- nommer un ASM;
- mettre en application la PSG, en promouvant un programme de sécurité doté d'une structure de gouvernance qui énonce clairement les responsabilités, ce qui permettra la gestion efficace de la sécurité au sein de l'Agence;
- donner son aval au plan de sécurité ministériel de l'ASFC, qui précise les décisions en matière de gestion des risques dans le domaine de la sécurité et qui décrit brièvement les stratégies, les buts, les objectifs, les priorités et les échéanciers en vue d'améliorer la sécurité à l'Agence, et de soutenir la mise en œuvre du plan;
- veiller à ce que tous les niveaux de direction de l'ASFC définissent et introduisent les exigences liées à la gestion de la sécurité et de l'identité dans les plans, les programmes, les activités et les services;
- garantir la prise de mesures correctives adéquates pour traiter des questions concernant la non-conformité à la politique, les allégations d'inconduite, les activités criminelles ou les incidents de sécurité présumés, notamment par le refus, la révocation ou la suspension des cotes de sécurité et de fiabilité, selon le cas.

## Vice-président (VP), Direction générale du contrôle

Le vice-président, Direction générale du contrôle, fournit une orientation fonctionnelle globale du programme de sécurité de l'Agence. Il soumet au président, au premier vice-président et au Comité exécutif les questions et les intérêts touchant la sécurité ayant une incidence importante sur la mission et les obligations de l'Agence.

Il incombe au vice-président, Direction générale du contrôle, de :

- veiller à l'établissement et à l'intégration des politiques, des procédures et des normes de sécurité dans le programme de sécurité de l'Agence;
- faire en sorte que les ressources pertinentes et nécessaires (financières, ressources humaines et biens) soient allouées au programme de sécurité;
- s'assurer que le programme de sécurité satisfait aux attentes en matière de rendement du président;
- garantir que le suivi et les comptes rendus appropriés sur le rendement du programme sont réalisés.







**Agent de sécurité du ministère (ASM)**

Le président de l'ASFC a nommé le directeur général de la Direction de la sécurité et des normes professionnelles à titre d'agent de sécurité du ministère (ASM). Il lui a délégué la responsabilité et l'autorité fonctionnelles de tous les aspects de la PSG, hormis les autorités désignées comme ne pouvant être déléguées selon la PSG.

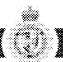
La gestion globale du programme de sécurité se résume comme suit :

- établir et diriger le programme de sécurité de l'Agence;
- gérer les relations nécessaires à la mise en œuvre des exigences de sécurité dans tous les secteurs qui assument des responsabilités relatives à la sécurité;
- veiller à ce que la gestion, la coordination et la mise en œuvre des exigences relatives à toutes les fonctions stratégiques du programme de sécurité de l'ASFC soient conformes à la PSG et à ses instruments de politique connexes;
- s'assurer de l'élaboration, de l'administration, de la gestion du risque et du contrôle efficaces des politiques et programmes de sécurité de l'Agence;
- veiller à ce que tous les membres de la haute direction de l'Agence soient au fait de leurs obligations de rendre compte et de leurs responsabilités à l'égard du programme de sécurité, et à ce qu'ils les intègrent à leurs politiques, normes, lignes directrices, procédures et bases de référence;
- faire en sorte que les obligations de rendre compte, les délégations, les liens hiérarchiques et les responsabilités des employés de l'Agence qui ont des répercussions sur la sécurité soient définis, consignés sur papier, et communiqués de manière adéquate;
- fournir une orientation fonctionnelle, des services de consultation et des lignes directrices destinés au réseau des praticiens de la sécurité de l'Agence;
- favoriser une culture de sécurité au sein de l'Agence;
- concevoir des séances de sensibilisation à la sécurité et en assurer la prestation auprès des employés et des gestionnaires à tous les échelons.

**Dirigeant principal de l'information (DPI)**

Le vice-président, Direction générale de l'information, des sciences et de la technologie, agit à titre de dirigeant principal de l'information pour l'Agence. Les responsabilités inhérentes à cette fonction consistent à :

- garantir la gestion efficace et efficiente de l'information et des biens en matière de TI de l'Agence;
- veiller à l'application des contrôles de sécurité appropriés à tous les biens de technologie de l'information (TI) et de gestion de l'information (GI) de l'Agence;
- assurer une relation productive et fonctionnelle entre le coordonnateur de la sécurité des TI (CSTI) et l'ASM, en vue d'établir une approche coordonnée et intégrée à l'égard de la mise en œuvre des exigences du programme de sécurité.



**Coordonnateur de la sécurité des TI (CSTI)**

Le coordonnateur de la sécurité des TI (CSTI) de l'ASFC entretient des liens hiérarchiques fonctionnels avec le DPI et l'ASM.

Il incombe au CSTI de :

- créer et gérer le programme de sécurité des TI de l'Agence, dans le cadre du programme de sécurité coordonné de l'Agence;
- passer en revue les politiques et normes de sécurité des TI et toutes les politiques ayant une incidence sur la sécurité des TI, et recommander leur approbation;
- veiller à la révision des sections portant sur la sécurité des TI dans les demandes de propositions et autres documents contractuels, incluant les listes de vérification des exigences relatives à la sécurité;
- recommander l'approbation de tous les contrats visant des fournisseurs externes des services de sécurité des TI;
- collaborer étroitement avec les gestionnaires chargés de la prestation des programmes et des services afin de :
    - veiller à ce que leurs besoins en matière de sécurité des TI soient satisfaits;
    - fournir des conseils sur les mesures de protection;
    - les informer de l'incidence possible des menaces nouvelles et existantes;
    - les conseiller sur le risque résiduel d'un programme ou d'un service.
- surveiller la conformité de l'Agence à la Gestion de la sécurité des technologies de l'information (GSTI) ainsi qu'aux normes et lignes directives connexes liées à la sécurité des TI;
- faire la promotion de la sécurité des TI à l'Agence;
- mettre en place un processus efficace pour le traitement des incidents de sécurité des TI et vérifier sa bonne application;
- faire office de principal agent de liaison de l'Agence pour les questions de sécurité des TI.

**Haute direction**

Il incombe à la haute direction (les vice-présidents, le premier vice-président et le président) de :

- fixer des objectifs pour le programme et d'assurer leur surveillance par l'entremise du Comité exécutif;
- garantir la sécurité des employés, des biens, de l'information et des services;
- veiller à l'observation de la politique, des normes et des pratiques de sécurité de l'Agence;
- veiller au suivi de l'observation de la politique, des normes et des pratiques de sécurité de l'Agence dans ses secteurs de responsabilité et au signalement à l'ASM de tout incident de sécurité ou de toute infraction à la sécurité;







- mettre en œuvre les exigences de sécurité particulières associées à leurs programmes opérationnels;
- promouvoir de façon constante une culture de sécurité au sein de l'Agence;
- faire en sorte d'intégrer les exigences du programme de sécurité dans la définition des priorités, de l'orientation stratégique, des objectifs de programme, du budget et des crédits de l'Agence;
- donner son approbation en ce qui a trait à toutes les politiques, normes et directives, en collaboration avec l'ASM, lorsqu'un élément de sécurité est en cause.

**Gestionnaires à tous les niveaux**

Il incombe aux directeurs généraux, aux directeurs, aux gestionnaires et à tous les autres niveaux de gestion à l'Administration centrale (AC) et dans les régions de :

- mettre en application les politiques, normes, directives et lignes directrices de sécurité dans leurs secteurs de responsabilité et de voir à ce que tous leurs employés délégués les comprennent et les observent;
- veiller à la protection des employés, de l'information, des biens et des services dont ils sont responsables;
- garantir l'intégration des exigences du programme de sécurité à la planification des activités, aux programmes, aux services et aux autres activités de gestion;
- veiller à la poursuite des activités dans leurs secteurs de responsabilité et au respect des exigences du programme de continuité des activités (PCA) de l'ASFC;
- procéder à l'évaluation des risques pour la sécurité, ainsi qu'au réexamen et à la réévaluation périodiques des risques par suite de modifications apportées aux programmes, aux activités ou aux services, tout en prenant des mesures correctives pour combler les lacunes cernées et renforcer la posture de sécurité de l'Agence;
- veiller à ce qu'aucun employé ne soit embauché ou nommé à un poste ou affecté à un poste intérimaire sans qu'il n'ait fait l'objet d'une enquête de sécurité et qu'on lui ait attribué la cote de sécurité exigée par l'ASFC;
- veiller à ce qu'une séance d'information sur la sécurité soit offerte à tous les employés au moment de l'embauche;
- suivre, tous les deux ans, tout comme leurs employés, les modules de formation obligatoires sur la sensibilisation à la sécurité offerts en ligne;
- surveiller le respect des politiques, des directives, des normes et des pratiques en matière de sécurité de l'Agence dans leur secteur de responsabilité;
- signaler les incidents de sécurité et les infractions à la sécurité;
- surveiller la mise en œuvre et l'efficacité des mesures de contrôle de sécurité, et en faire rapport à l'ASM au besoin.

**Employés à tous les niveaux**



Il incombe à tous les employés de l'Agence (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), aux contractuels et aux employés des agences privées ainsi qu'aux personnes en détachement ou affectées à l'ASFC (y compris les étudiants) de :

- classifier, désigner et marquer l'information ou les documents qu'ils créent afin de veiller à ce que des mesures de protection adéquates soient appliquées;
- protéger toute l'information et tous les biens sous leur contrôle, sur les lieux de travail et à l'extérieur;
- mettre en application et respecter les mesures de sécurité matérielle pour contrôler l'accès aux locaux, aux renseignements et aux biens de l'ASFC;
- mettre en application les contrôles de sécurité relatifs à leur secteur de responsabilité pour faire en sorte que les exigences de sécurité soient intégrées aux processus, aux pratiques et à l'exécution des programmes au quotidien;
- signaler les incidents de sécurité par les voies appropriées et suivre les directives de l'ASM s'il y a lieu;
- se tenir au courant des préoccupations et des enjeux liés à la sécurité, pour veiller à ce que leurs répercussions ne compromettent pas la posture de sécurité de l'Agence;
- se comporter au travail et à l'extérieur d'une manière qui n'entache pas l'intégrité de l'ASFC ou ne nuit pas à l'intégrité de l'ASFC;
- suivre (tous les deux ans) le module de formation obligatoire sur la sensibilisation à la sécurité offert en ligne et les autres formations obligatoires relatives aux pratiques de sécurité responsable.

**Praticiens de la sécurité**

Ce sont les personnes responsables de la coordination, de la gestion et de la fourniture de conseils et de services se rapportant aux activités de sécurité qui font partie intégrante d'un programme de sécurité ministériel coordonné, qui comprend entre autres, la sécurité de l'information, la sécurité des TI, la sécurité matérielle, les enquêtes de sécurité sur le personnel, la gestion des urgences, la planification de la continuité des activités et les opérations de sécurité régionales.

Il incombe aux praticiens de la sécurité de :

- préserver un rapport hiérarchique fonctionnel avec l'ASM, par l'entremise d'autorités fonctionnelles appropriées afin de veiller à la coordination et à l'intégration des activités de sécurité de l'Agence;
- sélectionner, mettre en œuvre et maintenir les contrôles de sécurité relatifs à leur secteur de responsabilité, pour veiller à la réalisation des objectifs de contrôle;
- surveiller et évaluer la mise en œuvre et l'efficacité des contrôles de sécurité, faire état de la réalisation des objectifs de contrôle à l'ASM, et recommander des mesures correctives pour combler les lacunes décelées dans les activités et les évaluations liées à la mesure du rendement;
- donner des conseils sur l'application et l'efficacité des contrôles de sécurité relatifs à leur secteur de responsabilité à l'intention de l'ASM, des gestionnaires à tous les niveaux et des employés;







- soutenir l'ASM dans l'élaboration et la prestation des séances de sensibilisation à la sécurité destinées aux employés et aux gestionnaires à tous les niveaux;
- participer aux évaluations des menaces et des risques et contribuer à l'élaboration du plan de sécurité de l'Agence (PSA), au besoin.



## 9. Conséquences

Le président doit s'assurer que des mesures correctives pertinentes sont prises pour résoudre les problèmes concernant le respect de la politique, les allégations de mauvaise conduite, les activités criminelles ou les incidents de sécurité présumés, y compris le refus, la révocation ou la suspension des cotes de sécurité, le cas échéant.

Les conséquences de l'inobservation des instruments de politique sur la sécurité de l'Agence peuvent comprendre :

- des suivis informels, des demandes de vérification interne ou des directives officielles de prise de mesures correctives;
- des mesures punitives ou administratives jugées adéquates dans les circonstances.

## 10. Annexes

Annexe A : Aperçu du programme de sécurité
Annexe B : Structure de responsabilisation du programme de sécurité de l'ASFC
Annexe C : Mandat du Comité de gestion de la sécurité

## 11. Références

**Lois liées à la présente politique (liste non exhaustive) :**

*Loi sur l'accès à l'information*
*Loi sur la preuve au Canada*
*Code canadien du travail*
Règlement canadien sur la santé et la sécurité au travail
*Charte canadienne des droits et libertés*
*Loi canadienne sur les droits de la personne*
*Loi sur le Service canadien du renseignement de sécurité*
Charte canadienne des droits et libertés
*Loi sur les douanes*
*Code criminel*
*Loi sur le casier judiciaire*
Loi sur la gestion des urgences
*Loi sur la gestion des finances publiques*
*Loi sur la Bibliothèque et les Archives du Canada*
*Loi sur la protection des renseignements personnels*
*Loi sur l'emploi dans la fonction publique*
*Loi sur les relations de travail dans la fonction publique*
*Loi sur la Gendarmerie royale du Canada*
*Loi sur la protection de l'information*
*Loi sur le système de justice pénale pour les adolescents*





**Politiques, directives et normes du Conseil du Trésor relatives à la présente politique (liste non exhaustive) :**

Politique sur l'accès à l'information
Directive sur la gestion de la sécurité ministérielle
Directive sur la gestion de l'identité
Directive sur les rôles et responsabilités en matière de gestion de l'information
Politique sur la protection contre les incendies, enquêtes et rapport
Politique sur la sécurité du gouvernement
Politique sur la gestion de l'information
Cadre de gestion intégrée du risque
Politique sur la vérification interne
Politique sur le contrôle interne
Politique sur les relations de travail
Politique en matière d'apprentissage, de formation et de perfectionnement
Directive sur les pertes de fonds et de biens
Politique sur la gestion des technologies de l'information
Politique sur la gestion du matériel
Politique sur la gestion des biens immobiliers
Politique sur la sécurité et la santé au travail
Norme de sécurité opérationnelle – Programme de planification de la continuité des activités (PCA)
Norme opérationnelle sur la sécurité matérielle
Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information
Norme sur le filtrage de sécurité
Politique sur la protection de la vie privée
Politique sur la gestion des projets
Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles
Conditions d'emploi (Politique)

**Autres documents relatifs au présent cadre :**

Code de valeurs et d'éthique de la fonction publique
Code de conduite de l'ASFC
Lignes directrices sur la communication des renseignements douaniers (Article 107 de la Loi sur les douanes)
Volume de sécurité de l'ASFC

## 12. Examen de la politique

Le Cadre de gestion du programme de sécurité sera examiné et révisé, le cas échéant, tous les ans pour tenir compte des changements organisationnels et des changements touchant le programme.



# 13.Demandes de renseignements

Pour obtenir de plus amples renseignements, veuillez communiquer avec :

Direction de la sécurité et des normes professionnelles
410, avenue Laurier, 9e étage
Ottawa (Ontario)
K1A 0L8
**Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca**







# Annexe A : Aperçu du programme de sécurité de l'ASFC

Le programme de sécurité de l'ASFC est une entité complexe qui est responsable de la prestation de tous les services de sécurité internes, c'est-à-dire la sécurité du personnel, la sécurité matérielle, la sécurité dans la passation de marchés, la sécurité de l'information y compris la sécurité des communications, la sécurité des TI, la gestion des installations qui traitent le renseignement spécial, l'élaboration de politiques sur la sécurité, la surveillance des activités de programme en lien avec la sécurité, les enquêtes sur les normes professionnelles, la gestion de la continuité des activités, la gestion des urgences, l'évaluation des risques liés à l'intégrité et l'orientation du programme d'intégrité. Le programme de sécurité de l'ASFC fournit des services de sécurité à près de 13 000 employés de l'Agence répartis dans environ 1 200 points de service au pays, englobant les points d'entrée des modes terrestre, aérien, ferroviaire et maritime, les passages à la frontière dans les régions éloignées, les points d'entrée sans personnel et les points de services à l'étranger.

Les activités du programme de sécurité sont régies par la *Politique sur la sécurité du gouvernement* (PSG) du Secrétariat du Conseil du Trésor (SCT), la *Directive sur la gestion de la sécurité ministérielle*, et la *Directive sur la gestion de l'identité*. Des exigences obligatoires supplémentaires sont énoncées dans les normes qui appuient les domaines suivants : la vérification de l'information et de l'identité, les enquêtes de sécurité sur le personnel, la sécurité matérielle, la sécurité des TI, la gestion des urgences et de la continuité des activités, ainsi que la sécurité en matière de passation de marchés.

Prise dans son sens le plus large, la sécurité du gouvernement est une garantie de protection des employés et des biens contre les préjudices. La mesure avec laquelle le gouvernement peut garantir sa propre sécurité influe directement sur sa capacité à assurer la protection des principaux biens et la prestation continue des services qui contribuent à la santé, au bien-être économique et à la sécurité de tous les Canadiens.

À l'ASFC, la gestion de la sécurité est un processus vivant et dynamique qui doit faire l'objet d'une évaluation constante et d'une gestion proactive des menaces internes et externes et des risques qui y sont associés. Cela comprend la mise en œuvre, la surveillance et le maintien de contrôles de gestion interne adéquats, notamment la prévention (atténuation), la détection, l'intervention et la reprise des activités. La gestion de la sécurité est en lien direct avec d'autres fonctions de gestion, dont l'accès à l'information et la protection des renseignements personnels, la gestion des risques, la gestion des urgences et de la continuité des activités, les ressources humaines, la santé et la sécurité au travail, l'immobilier, la gestion du matériel, la gestion de l'information, la technologie de l'information et les finances. À l'ASFC, la sécurité est à son mieux lorsqu'elle est intégrée à la culture et aux opérations au quotidien : c'est le seul moyen de garantir que le programme de sécurité aura une incidence favorable sur les employés et la direction.

Les exigences précisées dans le présent cadre forment la base d'une gestion efficace du programme de sécurité, qui permettra à l'ASFC de satisfaire à toutes les exigences de sécurité de la PSG ainsi qu'aux directives et aux normes connexes, tout en s'acquittant de ses obligations afférentes au programme de sécurité.







Toutes les directions générales appuient le programme de sécurité de l'ASFC. Toutefois, celui-ci est administré par la Direction de la sécurité et des normes professionnelles (DSNP) de la Direction générale du contrôle. Le président a désigné le directeur général de la DSNP à titre d'ASM à qui il a délégué la responsabilité et le pouvoir fonctionnels de tous les aspects de la PSG, notamment la gestion du programme de sécurité de l'ASFC. Alors que certains volets du programme exigent des connaissances spécialisées autres que celle de la Direction générale du contrôle [Direction générale de l'information, des sciences et de la technologie [DGIST] et Direction générale des opérations], globalement, la responsabilité et les obligations de rendre compte relatives au programme de sécurité relèvent de l'ASM. Veuillez consulter l'annexe B portant sur la structure de responsabilisation du programme de sécurité de l'ASFC.

## Objectifs du programme

L'ASFC se doit de mettre en œuvre un programme de sécurité rentable et efficient pour s'acquitter de ses responsabilités à l'égard de la population canadienne et pour se conformer à l'esprit, à l'intention et aux exigences de la PSG et de toutes les directives et normes connexes. L'ASFC doit également se conformer aux exigences juridiques et réglementaires applicables à l'Agence.

Ces énoncés de politique résument l'esprit, l'intention et les exigences de la PSG :

- l'information, les biens et les services ne sont pas compromis et les employés sont protégés contre la violence en milieu de travail;
- les structures de gouvernance, les mécanismes et les ressources sont en place pour assurer la gestion efficace et efficiente de la sécurité, tant au sein de l'Agence que dans l'ensemble du gouvernement;
- la gestion des incidents de sécurité est efficacement coordonnée au sein des ministères et dans l'ensemble du gouvernement;
- l'interopérabilité et l'échange de renseignements sont assurés au moyen de pratiques efficaces et uniformes en matière de gestion de la sécurité et de l'identité;
- la continuité des opérations et des services du gouvernement est assurée en cas d'incidents de sécurité, de perturbations ou de situations d'urgence.

**Définition des activités de sécurité**

La gestion de la sécurité peut être répartie entre les secteurs de programme de sécurité suivants :

**Administration de la sécurité et coordination du programme** – s'entend de la consignation par écrit des politiques, normes, lignes directrices et bases de référence sur les exigences en matière de sécurité interne et à l'établissement des mécanismes adéquats associés aux ententes concernant des biens ou des risques partagés entre divers organismes.

**Sensibilisation à la sécurité et formation en matière de sécurité** – comprend deux volets. D'une part, la sensibilisation à la sécurité vise à veiller à ce que l'ensemble du personnel de l'ASFC ait été informé de ses responsabilités concernant la protection des employés, de l'information et des biens. D'autre part, la formation en matière de sécurité correspond à la fourniture de connaissances techniques en vue de satisfaire au Conseil du Trésor ainsi qu'aux différentes exigences réglementaires et aux normes des tribunaux.







**Sécurité matérielle** – s'entend de la protection physique, technique, procédurale et psychologique appropriée des personnes et des biens matériels (biens, installations, infrastructures, etc.).

**Signalement des incidents de sécurité** – comporte l'identification, l'enquête, les comptes rendus, le traitement et l'analyse en lien avec les évènements associés à des infractions à la sécurité, à la perte ou à des préjudices aux biens, à la confidentialité, à l'intégrité ou à l'accessibilité, et à la valeur relative ou à la confiance du public accordée aux employés de l'Agence, aux biens de nature délicate ou aux opérations.

**Sécurité de l'information (InfoSec)** – veille à que les mesures de protection physique, technique, procédurale et psychologique soient appliquées à l'information (sous toutes ses formes), de sa conceptualisation à sa destruction définitive et irrévocable. Il est à remarquer que la sécurité de l'information se servira des intrants de nombreuses autres entités, plus particulièrement de la sécurité informatique, de la sécurité matérielle et de la sécurité du personnel.

**Sécurité des communications (COMSEC)** – concerne l'application de mesures de sécurité cryptographique, de sécurité des transmissions et des émissions et de sécurité matérielle ainsi que de pratiques et de mécanismes de contrôle opérationnels pour empêcher tout accès non autorisé à l'information issue de télécommunications et pour garantir l'authenticité de ces télécommunications.

**Agent de surveillance du renseignement sur les communications (COMCO)** –responsable de la gestion et de la supervision de l'information classifiée et sensible d'intérêt pour le renseignement national et définie et désignée comme documents spéciaux. Les documents spéciaux représentent toute information ou tout document exigeant une surveillance particulière pour en garantir la manipulation restreinte, au moyen des systèmes compartimentés du renseignement étranger. Les documents spéciaux comprennent entre autres le renseignement d'origine électromagnétique (SIGINT).

**Gestion de l'identité** – ensemble de principes, pratiques, processus et procédures servant à l'exécution du mandat et à la réalisation des objectifs relatifs à l'identité d'un organisme.

**Sécurité du personnel** – observation des normes de conduite appropriées et examen de la fiabilité et évaluation de la loyauté en vue d'établir la cote de sécurité (fiabilité, Secret ou Très secret) de toutes les personnes qui ont un accès aux infrastructures de l'Agence (installations, biens, systèmes informatiques, etc.).

**Enquêtes visant les normes professionnelles** – enquêtes sur des doutes ou des allégations d'inconduite des employés en service ou non à l'égard du *Code de conduite* de l'ASFC, du *Code de valeurs et d'éthique de la fonction publique*, des politiques de l'ASFC, des violations au droit criminel ou aux autres lois et règlements.

**Sécurité des technologies de l'information (ITSec)** – mesures de protection opérationnelles, administratives, techniques et logiques appliquées aux appareils ou à d'autres biens servant à communiquer de l'information sous diverses formes, avec un accent particulier sur l'application, la conception, la configuration et l'utilisation adéquate de la technologie.







**Gestion des urgences** – gestion des urgences concernant tous les dangers, notamment l'ensemble des activités et des mesures de gestion des risques en lien avec la prévention et l'atténuation, la préparation aux situations d'urgence, l'intervention et la reprise des activités.

**Planification de la continuité des opérations (PCO)** – élaboration et exécution rapide de plans, mesures, procédures et ententes veillant à une interruption minimale ou nulle de l'accessibilité aux services et aux biens essentiels en cas d'évènements importants perturbateurs pour les activités de l'Agence. Cela comprend :

- les mesures associées à la prévention et à la détection, aux notifications et aux interventions relatives aux activités, dans le cadre des modèles de planification de la continuité des opérations;
- les mesures associées à la prévention, à la préparation, à la détection, aux notifications, à l'atténuation des risques et aux interventions dans le cadre des modèles de préparation aux situations d'urgence.

**Planification de la continuité des TI** – élaboration et exécution rapide de plans, mesures, procédures et ententes veillant à une interruption minimale ou nulle de l'accessibilité aux services de TI, aux systèmes, aux données et aux infrastructures en cas d'évènements importants perturbateurs pour les activités de l'Agence.

**Santé et sécurité** – mise en place d'un programme conforme à la partie II du *Code canadien du travail* afin de faire en sorte que les employés travaillent dans un milieu sain et sécuritaire.

## Administration de la sécurité

L'administration du programme de sécurité de l'ASFC repose sur les principes de la PSG, de la *Directive sur la gestion de la sécurité ministérielle*, et de la *Directive sur la gestion de l'identité*. Chacun de ces instruments exige l'intégration des notions suivantes au programme :

1. ***Planification;***
2. ***Gouvernance;***
3. ***Gestion des risques en matière de sécurité;***
4. ***Surveillance et contrôle;***
5. ***Mesure et évaluation du rendement;***
6. ***Soutien à l'échelle du gouvernement.***

## 1. Planification

La planification de la sécurité de l'Agence, qui mène finalement à la définition des priorités globales du programme de sécurité, s'articule autour de l'évaluation continue des risques internes et externes et de leurs répercussions potentielles sur l'ASFC. Par le passé, plusieurs activités de sécurité étaient exécutées en réaction aux priorités du gouvernement du Canada et de l'Agence.

Grâce à une planification consciencieuse, l'organisation de la sécurité a évolué et s'est renforcée au fil du temps. Le plan de sécurité de l'Agence repose sur les efforts importants qui ont été investis







dans les analyses des écarts et l'exposition aux risques. Ce plan décrit les méthodes de gestion des risques pour la sécurité et résume les stratégies, les buts, les objectifs et les échéanciers visant l'amélioration de la posture de sécurité globale de l'Agence.

Le Plan de sécurité de l'Agence :

- fournit une vision uniformisée des exigences en matière de sécurité de l'Agence;
- cerne les menaces à la sécurité, les risques et les vulnérabilités pour définir un ensemble approprié d'objectifs de contrôle;
- détermine et établit des contrôles supplémentaires en vue d'atteindre les objectifs de contrôle et un niveau acceptable de risques résiduels;
- décrit brièvement les stratégies, les objectifs et les priorités en matière de sécurité ainsi que les délais connexes pour améliorer la posture de sécurité de l'Agence;
- définit les processus, les rôles et les responsabilités en ce qui a trait à l'évaluation du rendement, de l'information et des réalisations.

## 2. Gouvernance

Le Comité de gestion de la sécurité (CGS) (annexe A] a été établi comme le centre de consultation et de gouvernance dans les domaines de la sécurité, de la gestion des urgences et de la planification de la continuité des activités. Il relie les trois directions générales ayant des rôles fonctionnels, opérationnels et de sécurité (DGIST, Direction générale des opérations et Direction générale du contrôle) aux directions générales ayant un rôle de sécurité indirect et accessoire (Direction générale des programmes, Direction générale des ressources humaines et Direction générale des services intégrés). Les membres du CGS représentent tous les secteurs de l'ASFC (y compris les directeurs régionaux des services organisationnels et des programmes) qui jouent un rôle dans la prestation du programme de sécurité. Ce comité est présidé par l'ASM.

Les membres du CGS sont responsables de la coordination et de l'intégration des activités de sécurité aux opérations, plans et priorités de l'Agence, et doivent fournir des services de consultation et du soutien dans ces domaines à l'intention des comités suivants :

- Comité de gestion de l'Agence (CGA);
- Comité exécutif (CE)

De plus, les gestionnaires de la sécurité assistent à des téléconférences bimensuelles pour discuter des questions de l'Agence relatives à la sécurité, auxquelles participent les gestionnaires régionaux de la sécurité et les gestionnaires de la sécurité à l'AC. Y sont invités à l'occasion des représentants d'autres secteurs de programme de l'ASFC.

De surcroît, le Groupe de travail sur la sécurité, les opérations et la continuité (GTSOC) a été formé pour agir à titre d'organisme consultatif dans les domaines de la sécurité ministérielle, des opérations, de la continuité des activités et pour fournir des conseils et des comptes rendus sur la situation au CGS au cours et à la suite d'évènements importants.



Pour veiller à la coordination des activités du programme de sécurité au sein de l'ASFC et de l'appareil gouvernemental, le personnel de la sécurité à divers niveaux participe à plusieurs comités internes et externes et groupes de travail.

**3. Gestion des risques en matière de sécurité**

La gestion des risques en matière de sécurité est une approche systématique à l'égard de l'évaluation des menaces, de l'analyse des risques et de la mise en œuvre des contrôles. Les principales étapes du processus comprennent la détermination, l'examen, l'évaluation et le traitement des risques pour la sécurité. Étant donné qu'elles constituent le cœur même des exigences du programme de sécurité, il importe que ces étapes s'inscrivent dans le cycle de vie.

L'Agence est responsable de l'élaboration, de l'enregistrement, de l'application et de la mise à jour des processus nécessaires à la gestion systématique des risques pour la sécurité, pour veiller à les adapter continuellement en fonction de l'évolution des besoins de l'Agence et du contexte des menaces.

On y parvient grâce à l'approche intégrée d'équipes multidisciplinaires responsables de la gestion de ces processus, lesquels sont mis en œuvre par la Section de la sécurité à l'Administration centrale (AC) et par les bureaux régionaux de la sécurité. La section qui suit approfondira la définition des composantes connexes du programme ci-dessous et leur contribution à la gestion globale des risques pour la sécurité :

- Administration de la sécurité et coordination des programmes;
- Politique sur la sécurité, sensibilisation et formation;
- Sécurité matérielle;
- Sécurité de l'information (incluant la sécurité des communications);
- Sécurité des technologies de l'information;
- Gestion de l'identité;
- Enquêtes de sécurité sur le personnel;
- Intégrité professionnelle;
- Enquêtes visant les normes professionnelles;
- Sécurité à l'AC et dans les régions
- Gestion des urgences;
- Gestion de la continuité des activités;
- Gestion de la continuité des technologies de l'information (TI);
- Santé et sécurité.

**Administration de la sécurité et coordination des programmes**
**Politique sur la sécurité, sensibilisation et formation**

La *Section de la politique sur la sécurité et de la coordination de programme*, en collaboration avec les autorités fonctionnelles, assure la coordination centrale et la fonction de gouvernance requises pour assurer de manière efficiente et efficace la prestation des



services de sécurité et pour répondre aux différentes exigences découlant des organismes centraux ou des organismes responsables.

La sensibilisation à la sécurité vise à faire en sorte que tous les membres du personnel de l'ASFC connaissent leurs responsabilités en matière de protection des employés, de l'information et des biens, alors que la formation sur la sécurité permet l'acquisition des connaissances techniques, des habiletés et des aptitudes nécessaires à l'exécution des tâches relatives à la sécurité (soit la prestation du programme de sécurité de l'ASFC).

Les activités sont les suivantes :

- veiller à ce que les politiques, les directives, les normes, les lignes directrices et les procédures de sécurité de l'ASFC soient conformes à la PSG;
- élaborer et mettre en œuvre le plan de sécurité de l'Agence, assurer son suivi et produire les rapports connexes;
- coordonner les activités de communication régulières liées à la gestion de la sécurité à l'Administration centrale (AC) et dans les régions;
- passer en revue les ententes de collaboration écrites (c'est-à-dire les PE, les échanges de lettres) afin de garantir qu'elles respectent les exigences en matière de sécurité;
- coordonner et préparer les réponses aux documents de planification et de rapport :
    - le Cadre de responsabilisation de gestion (CRG);
    - le plan des risques d'entreprise (PRE);
    - les vérifications internes et externes.
- coordonner les exigences inhérentes à la formation et à la sensibilisation liées à la sécurité;
- promouvoir la sensibilisation et coordonner les activités de formation et les produits connexes;
- tenir à jour les dossiers sur la sensibilisation et la formation;
- assurer la sensibilisation à la sécurité par l'entremise de la formation et de la promotion.

**Sécurité matérielle**

La politique relative à la sécurité matérielle décrit les buts, les objectifs, les activités principales et les responsabilités liés au programme de sécurité matérielle au sein de l'ASFC.

La sécurité matérielle est fondée sur la théorie selon laquelle la conception externe et interne d'une installation et des contrôles de sécurité particuliers peut créer un environnement où les objectifs suivants sont atteints :

- le risque de violence à l'égard des employés est réduit;
- le risque d'accès non autorisé à des biens de nature délicate est réduit;
- le risque de perturbation des activités de l'Agence est réduit.

À cette fin, on prend ou on applique certaines mesures qui visent à préserver le caractère confidentiel, l'intégrité, la disponibilité et la valeur des biens de l'ASFC. Ces mesures sont des contrôles de sécurité qui sont généralement organisés sous forme de contrôles administratifs (notamment des politiques, des normes, des procédures, etc.), de contrôles physiques (barrières, éclairage, avertisseurs, matériel vidéo en circuit fermé, contenants, etc.), de







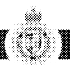
contrôles procéduraux (contrôles d'intégrité effectués par deux personnes et enregistrement de l'accès) et de contrôles techniques (pratiques de conception). Ces contrôles sont regroupés dans des systèmes de protection.

**Sécurité de l'information**
L'un des principes directeurs de la PSG est la protection de l'information contre la compromission accidentelle ou délibérée. L'information est cruciale à l'exécution des opérations. Par conséquent, sa confidentialité, son intégrité et son accessibilité revêtent la plus haute importance.

La *Section de la sécurité de l'information* est responsable de la mise en œuvre des processus de sécurité relatifs à la protection de l'information de l'Agence, peu importe son format (papier ou électronique), et, dans une certaine mesure, des systèmes (matériel et logiciels) qui soutiennent celle-ci. Il convient de noter que la Sécurité de l'information se servira des intrants de nombreuses autres entités, plus particulièrement de la sécurité des TI, de la sécurité matérielle et de la sécurité du personnel.

Les activités sont les suivantes :

- contrôler et surveiller le programme grâce à l'assistance et aux conseils des intervenants de l'ASFC en ce qui a trait à la sécurité de l'information, et assurer le suivi de l'efficacité des contrôles de sécurité;
- gérer les risques par l'entremise de l'élaboration, de la documentation, de la mise en œuvre et de la mise à jour des processus pour la gestion systématique des risques de sécurité liés à l'information;
- aider à conserver l'intégrité de tous les fonds de renseignements de l'Agence et la sécurité de ces systèmes;
- participer à l'évaluation de la sécurité et aux autorisations des systèmes d'information qui appuient les pratiques de gestion du risque, en examinant les évaluations de la menace et du risque et d'autres documents en vue de cerner correctement les risques liés à la confidentialité, à l'intégrité et à la disponibilité des fonds de renseignements;
- gérer l'administration, la distribution et le soutien des biens de la sécurité des communications;
- gérer les renseignements classifiés et de nature délicate en lien avec les intérêts nationaux du renseignement (contrôle du renseignement des communications) et en assurer la surveillance;
- assurer une surveillance de l'intégrité, c'est-à-dire :
  - coordonner les activités de surveillance du réseau et des bases de données (p. ex. courriel, utilisation du Web, entreposage des systèmes);
  - assurer la tenue des enquêtes TI et le soutien à la surveillance du réseau en ce qui concerne les enquêtes sur les normes professionnelles;
  - coordonner et approuver les demandes d'accès au Web, et surveiller l'utilisation du Web.
- agir à titre d'autorité en matière de communication de renseignements à des tiers demandeurs (p. ex. extraits de bases de données, courriels et dossiers des employés);
- effectuer des vérifications au chapitre de la sécurité des bases de données (p. ex. Centre d'information de la police canadienne).



**Sécurité des technologies de l'information (TI)**
Le programme de sécurité des TI est une sous-composante du programme de sécurité de l'Agence. Il est géré par la Division de la sécurité et de la continuité des opérations des TI (DSCOTI) de la Direction générale de l'information, des sciences et de la technologie (DGIST). Bien que la DGIST assume la responsabilité fonctionnelle des activités de sécurité précisées dans la section suivante, l'ensemble de la planification, des politiques et des efforts est coordonné et harmonisé au programme global de sécurité de l'Agence, sous la direction de l'ASM.

Un coordonnateur de la sécurité des TI (CSTI) doit maintenir un lien hiérarchique fonctionnel avec l'ASM. Les rôles en matière de la sécurité des TI sont précisés tout au long du présent cadre et dans le Volume de sécurité de l'Agence. La Direction de la sécurité et des normes professionnelles (DSNP) et le CSTI ont élaboré une entente de gouvernance du programme de sécurité informatique (Annexe B) détaillée, qui établit le cadre de gouvernance pour la prestation des services de sécurité des TI.

Le programme de sécurité des TI, qui repose sur la charte du programme de sécurité des TI, est structuré en vue d'appuyer la prestation des services de sécurité des TI dans les domaines d'importance qui suivent :

La *Section d'évaluation du risque et de consultation (ERC)* collabore avec les clients de l'ASFC pour s'assurer que les applications et les systèmes de l'Agence sont élaborés et mis en œuvre selon les niveaux approuvés et adéquats de contrôle de sécurité des TI, qui garantissent que les systèmes, l'information et les données de l'organisation sont protégés contre la divulgation non autorisée, le mauvais emploi ou l'accès non autorisé.

L'ERC utilise des outils d'évaluation pour effectuer des analyses et déterminer s'il y a des besoins en matière de sécurité des TI.

L'ERC évalue les risques liés à la sécurité des TI par rapport aux systèmes des TI de l'ASFC, aux applications et aux données. L'ERC fournit une orientation et formule des recommandations qui permettront l'atténuation des risques à un niveau jugé acceptable.

Les activités sont les suivantes :
- l'harmonisation avec la vision et la mission de l'Agence, soit de fournir, de façon optimale et fiable, des services frontaliers intégrés à l'appui des priorités liées à la sécurité nationale et à la sécurité publique;
- la protection de l'information et des données de l'ASFC contre toute compromission ou tout accès non autorisé, conformément aux politiques de l'Agence et à la *Politique sur la sécurité du gouvernement*.

La *Section du Centre de cyberprotection de la sécurité des TI* est responsable de l'établissement et du maintien d'une gestion uniforme de la sécurité des TI, des services et des projets connexes. Le Centre respecte les directives fournies par les organisations gouvernementales clés, notamment la *Norme opérationnelle de sécurité sur la gestion de la sécurité des technologies de l'information* (GSTI) du Secrétariat du Conseil du Trésor.







Le Centre de cyberprotection veille à ce que l'ASFC ait des processus et des procédures en place pour être en mesure d'intervenir rapidement en cas de cyberévènements ou de cyberincidents susceptibles d'avoir des répercussions négatives sur les biens de TI.

Le Centre de cyberprotection est responsable de la surveillance des cyberalertes recensées par le Centre canadien de réponse aux incidents cybernétiques (CCRIC), et des interventions s'y rattachant. Cela comprend la coordination avec les partenaires dans le domaine de la sécurité, dont le Centre de la sécurité des télécommunications Canada, Services partagés Canada, l'Agence du revenu du Canada (ARC) et la Gendarmerie royale du Canada (GRC), et ce, dans le but :

- de contenir et d'atténuer les menaces possibles;
- d'intervenir dans le cadre de cyberincidents et de le faire en temps opportun;
- de fournir des comptes rendus aux membres de la direction afin de les tenir informés de la situation et de trouver une solution visant à réduire le niveau de risque.

Le Centre de cyberprotection offre des services techniques, notamment des évaluations et des recommandations en matière de solutions de sécurité (p. ex. recherche de solutions sécuritaires quant à l'utilisation d'iPad à l'Agence). Les solutions peuvent comprendre l'évaluation et la mise à l'essai de produits. En outre, le Centre offre des services d'évaluation des vulnérabilités pour les systèmes et les applications.

Les activités de la *Section de gouvernance et de stratégie* poursuivent un objectif stratégique, qui complète le volet opérationnel de la sécurité des TI, dont sont responsables d'autres sections de la DSCOTI.

Plus particulièrement, la Section de gouvernance et de stratégie offre des services de planification et de rapports au titre du programme de sécurité des TI de l'ASFC, en plus de participer de manière importante au processus d'élaboration des normes et de la politique de l'Agence afférentes à la sécurité des TI ainsi que des programmes de formation et de sensibilisation à la sécurité des TI.

Les activités sont les suivantes :

- fournir des conseils et des directives relativement aux demandes de renseignements sur la sécurité des TI, dont l'interprétation de la politique;
- offrir, au besoin, des séances de sensibilisation personnalisées sur la sécurité des TI, en complément des modules de formation en ligne obligatoires.

La Section de gouvernance et de stratégie assure la liaison avec les intervenants de l'ASFC pour veiller à ce que les programmes stratégiques en matière de sécurité des TI soient continuellement harmonisés aux besoins opérationnels de l'Agence. La section collabore aussi étroitement avec la Direction de la sécurité et des normes professionnelles de la Direction générale du contrôle.

**Gestion de l'identité**

La gestion de l'identité est un élément précis et fait partie intégrante des programmes, services et activités des ministères. Elle est au cœur de l'administration publique et de la majorité des processus opérationnels de l'Agence. Après l'établissement d'une identité, toutes les activités







gouvernementales ultérieures, de la protection des biens à la prestation des services, en passant par les droits et les interventions en cas d'urgence, reposent sur cette identité.

Il faut adopter une approche plus globale en matière de gestion de la sécurité. On s'assure ainsi de satisfaire aux exigences de sécurité et de mettre sur pied, d'administrer et de fournir des services aux bons clients. L'élaboration et la mise en œuvre de cette approche normalisée permettront également l'établissement d'une solution robuste, évolutive et flexible pour la validation adéquate de l'information d'identification.

*Il incombe aux gestionnaires de tous les niveaux de :*

- s'assurer que la nécessité de l'identification est justifiée et que l'on est légalement habilité à procéder à une vérification d'identité pour le besoin d'un programme particulier ou à l'appui des activités d'exécution de la loi, de sécurité nationale ou de défense;
- signaler les risques pour la gestion de l'identité (p. ex. changement de situation, erreurs, méfaits), les incidences sur les programmes, les niveaux d'assurance requis et les options d'atténuation des risques;
- sélectionner un ensemble pertinent de données d'identité (comme des caractéristiques personnelles ou des données d'identification), qui est suffisant pour établir une identité unique afin de répondre aux besoins des programmes, qui est proportionnel aux risques recensés et qui est assez souple pour permettre la mise en place d'autres méthodes d'identification au besoin;
- mettre en œuvre des solutions d'échange d'information d'identification respectueuses des normes courantes au gouvernement du Canada.

*Il incombe aux gestionnaires des ressources humaines de* :

- faire en sorte que les employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel, étudiants, contractuels, employés temporaires des agences privées, notamment le personnel muté, détaché ou affecté) se voient tous attribuer un code d'identification de dossier personnel (CIDP) pour la gestion de l'information et des opérations relatives aux employés;
- veiller à ce qu'un numéro individuel d'organisme (NIO) soit attribué à chaque employé dont l'identité doit être établie auprès d'un ou de plusieurs organismes de remise à l'extérieur de la fonction publique fédérale.

**Enquêtes de sécurité sur le personnel**

Tous les individus dont on envisage l'embauche à l'Agence doivent faire l'objet d'une enquête de sécurité sur le personnel afin d'obtenir une cote de fiabilité et, si le poste l'exige, une cote de sécurité, avant d'être nommés à un poste. Ce processus est appuyé par la *Section des enquêtes de sécurité sur le personnel.*

Les activités sont les suivantes :

- surveiller la conduite de toutes les activités liées aux enquêtes de sécurité sur le personnel;
- assurer le suivi des examens justifiés et des révocations dans le cas où des renseignements défavorables compromettent la cote de sécurité d'une personne;
- formuler des recommandations auprès de l'agent de sécurité du ministère sur la délivrance des cotes de sécurité;





- conserver des dossiers sur les enquêtes de sécurité du personnel pour tous les employés de l'ASFC;
- diriger la conduite des évaluations de la fiabilité – vérifier la loyauté, l'honnêteté, l'intégrité et la fiabilité, ce qui nécessite de procéder à des vérifications de solvabilité et du dossier judiciaire et à d'autres vérifications approfondies, dont les entrevues sur l'intégrité;
- coordonner les évaluations du Service canadien du renseignement de sécurité (SCRS) pour établir la loyauté d'une personne envers le Canada relativement aux demandes de cotes de sécurité Secret et Très secret;
- fournir une orientation fonctionnelle et stratégique pour les praticiens régionaux de la sécurité.

**Programme d'intégrité professionnelle**

Le Programme d'intégrité professionnelle (PIP) a été mis en place pour promouvoir l'intégrité professionnelle parmi ses employés et une approche concertée à l'égard de la gestion des risques liés à l'intégrité professionnelle. Au sens de l'ASFC, l'intégrité professionnelle signifie que ses employés se doivent :

- d'exercer leur autorité avec honnêteté, ouverture et équité;
- d'être responsables de leurs actes pour se forger et maintenir une réputation de loyauté et de responsabilité;
- de traiter les autres avec respect;
- d'agir comme il se doit même lorsque personne ne les surveille;
- protéger les biens matériels et informationnels de l'ASFC.

Les activités sont les suivantes :

- accroître la sensibilisation à l'intégrité professionnelle à la grandeur de l'ASFC;
- communiquer clairement et renforcer les normes attendues de conduite professionnelle de tous les employés de l'AFSC, pendant et après les heures de travail;
- faire en sorte que les employés de l'AFSC sachent comment détecter, signaler, éviter et atténuer les cas d'inconduite;
- mener des activités de surveillance pour veiller à ce que les risques pour l'intégrité professionnelle soient cernés, signalés, surveillés en permanence et atténués.

**Enquêtes visant les normes professionnelles**

Tous les organismes établissent des normes de comportement et de conduite que leurs employés doivent incarner et respecter. À l'ASFC, ces normes sont résumées dans le *Code de conduite*, un prolongement du *Code de valeurs et d'éthique de la fonction publique*, parmi les autres instruments stratégiques.

Ces codes informent les employés sur le comportement que l'on attend d'eux, au travail et à l'extérieur, soit une conduite sans reproche et respectueuse des politiques et des procédures du gouvernement. Les manquements relatifs à ces attentes peuvent être considérés comme une inconduite.

L'inconduite s'entend de toute action ou inaction commise par un employé, qu'il soit ou non de service, et par lequel il contrevient à une loi (y compris le *Code criminel du Canada*), à un règlement, à une règle, à une politique de l'ASFC, à une procédure approuvée ou au *Code de conduite de l'ASFC*,



ou par lequel il participe à une activité qui jette le discrédit sur l'ASFC ou qui nuit aux liens étroits qu'entretient l'ASFC avec d'autres organismes d'exécution de la loi.

Lorsque de l'information défavorable concernant un employé de l'ASFC est divulguée à la Division de la sécurité du personnel et des normes professionnelles ou découverte par celle-ci, la *Section d'analyse de sécurité et des normes professionnelles* de la Division de la sécurité du personnel et des normes professionnelles est responsable des éléments suivants :

- procéder à des évaluations préliminaires des faits divulgués pour déterminer la probabilité que l'inconduite ou le méfait allégué se soit produit ou va se produire, la gravité de l'inconduite ou du méfait allégué et la présence de motifs pouvant donner lieu à une enquête administrative (enquête relative à un examen justifié, enquête sur les faits, enquête sur les normes professionnelles);
- fournir une orientation, un soutien et un suivi quant à l'état des enquêtes sur les faits menées par la direction locale, évaluer les rapports de l'évaluation préliminaire effectuée par la direction locale et leurs conclusions;
- veiller au suivi des dossiers communiqués et des rapports d'état, notamment les évaluations préliminaires, les refus, les renvois et les enquêtes en cours;
- gérer et tenir à jour une base de données alimentée par des données des rapports pertinents relatifs à toutes les divulgations, enquêtes, conclusions et mesures de suivi;
- fournir des statistiques à jour sur les divulgations, les enquêtes, les conclusions et les mesures de suivi aux fins d'analyse, de planification et de mesure du rendement;
- tenir des séances d'information annuelles et semestrielles sur les tendances des enquêtes relatives à l'inconduite à l'intention du Comité exécutif.

À cette fin, la *Section des enquêtes visant les normes professionnelles* est responsable des éléments suivants :

- assurer la prestation de services d'enquête administrative centralisée et indépendante pour la haute direction de l'ASFC;
- mener des enquêtes sur les allégations d'inconduite des employés au travail et à l'extérieur, telles les violations du *Code de conduite de l'ASFC,* du *Code de valeurs et d'éthique de la fonction publique* et d'autres politiques gouvernementales;
- produire des rapports sur les constatations et les conclusions relatives à l'inconduite alléguée;
- rendre compte aux organismes d'exécution de la loi et assurer la liaison avec ceux-ci en ce qui concerne les infractions criminelles alléguées mettant en cause des employés de l'ASFC;
- présenter un témoignage lors de procédures devant les tribunaux administratifs ou la cour;
- formuler des observations à la haute direction sur les lacunes ou les faiblesses décelées dans les politiques ou les procédures par suite d'une enquête.

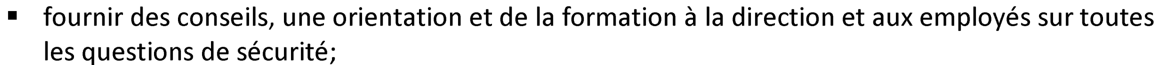
**Sécurité à l'AC et bureaux régionaux de sécurité – Prestation des programmes**

La *Section de la sécurité à l'Administration central*e et les *bureaux régionaux de sécurité* ont la responsabilité de fournir des conseils et une orientation au personnel des régions et de l'AC pour veiller à ce que la posture de sécurité matérielle des lieux occupés par l'ASFC protège adéquatement les employés, l'information et les biens de l'Agence.

Les activités sont les suivantes :





- fournir des conseils, une orientation et de la formation à la direction et aux employés sur toutes les questions de sécurité;
- fournir de la formation, des conseils et une orientation en lien avec les équipes et les plans d'évacuation des immeubles;
- veiller à ce que des mesures soient en place pour la protection des employés lorsque des occupations, des manifestations, des menaces à la bombe, des incendies ou des actes de violence peuvent se produire (c'est-à-dire, disposer de plans d'évacuation d'urgence à jour);
- mener des inspections ou examens de sécurité des installations nouvelles ou existantes pour évaluer la posture de sécurité, cerner les faiblesses et formuler des recommandations ou des spécifications en matière de sécurité et, une fois les recommandations mises en œuvre, approuver l'installation;
- assurer la prestation de services centralisés et veiller à la protection et au contrôle adéquats de tous les biens contrôlés (équipement lié à la sécurité des communications, insignes, armes à feu, cartes d'identité et d'accès);
- exécuter les fonctions de vérification et de surveillance concernant les biens contrôlés (les salles d'armement);
- coordonner toutes les demandes d'enquêtes de sécurité sur le personnel qui ont été présentées;
- procéder à des évaluations de la menace et des risques, à des examens sur place et à des ratissages de sécurité;
- assurer la coordination des mises à l'essai, de l'entretien et de la surveillance des systèmes de contrôle de l'accès électronique et d'alerte en cas d'intrusion;
- veiller à ce que le programme national de sécurité matérielle soit mis en œuvre et respecté;
- veiller à l'inclusion des exigences de sécurité dans tous les marchés de l'AC, offrir des conseils et une orientation, et agir à titre d'autorité d'approbation de la liste de vérification des exigences relatives à la sécurité conformément au pouvoir délégué par l'ASM;
- administrer un réseau de signalement des incidents de sécurité, mener des enquêtes et rédiger les rapports relatifs aux incidents, atteintes et violations en lien avec la sécurité, et recommander des mesures correctives à la direction;
- offrir des services d'agent en chef des opérations pendant les heures de fermeture et répondre aux appels (alertes d'intrusion, demandes des gardiens relatives à l'accès, aide aux employés, etc.);
- mettre à jour la ligne d'information pour les employés en cas d'urgence, en fonction des fermetures d'installations ou de perturbations au sein de celles-ci;
- tenir un inventaire de tous les cadenas à combinaison, veiller à l'étiquetage et au dénombrement de toutes les armoires et de tous les cadenas, ainsi qu'à l'exécution des demandes de changement de combinaison;
- participer et assurer une représentation aux comités sur la sécurité, au besoin (p. ex. organisation de secours de l'immeuble, santé et sécurité au travail).

**Gestion des urgences**

**La Direction générale du contrôle**

La gestion des urgences concerne la gestion de tous les dangers, y compris l'ensemble des activités et des mesures de gestion des risques en lien avec la prévention, l'atténuation, la préparation, l'intervention et le rétablissement.





Les activités sont les suivantes :

- assurer une surveillance des programmes stratégiques du Programme intégré de gestion des urgences de l'ASFC [y compris la sécurité, la gestion des urgences (Direction générale des opérations), le Centre des opérations frontalières, les TI, la gestion de la continuité des opérations, les ressources humaines, les communications et les services juridiques];
- diriger et coordonner l'établissement de cadres intégrés de gestion des urgences;
- élaborer, mettre en œuvre et tenir à jour le Plan stratégique de gestion des urgences (PSGU) de l'ASFC ainsi que le Registre des risques liés à la gestion des urgences (RRGU);
- assumer la responsabilité de la surveillance, de la contribution et du contrôle d'un calendrier détaillé des exercices de l'ASFC intégrant des exercices de préparation opérationnelle, de planification de la continuité des activités et de continuité des TI;
- gérer et mettre à jour la ligne d'information pour les employés de l'Agence (LIE) de la région de la capitale nationale (RCN).

**Direction générale des opérations, Centre national des opérations frontalières (CNOF)**

L'*Unité de la gestion des urgences* assure la surveillance des programmes et fournit des directives sur les mesures de gestion des urgences opérationnelles. Elle maintient l'état de préparation opérationnelle et coordonne avec les partenaires du gouvernement du Canada appropriés, notamment le Centre des opérations du gouvernement et autres intervenants concernant les initiatives de sécurité intergouvernementales, comme le Plan fédéral d'intervention d'urgence (PFIU), le Protocole d'intervention d'événement maritime (PIEM) et autres.

Les activités sont les suivantes :

- Assurer la gestion des programmes en ce qui concerne les mesures de gestion des urgences opérationnelles et aider les régions à établir et à tenir des plans de gestion des urgences, des plans de continuité des activités pour les points d'entrée, des plans pour le Centre des opérations régionales (COR), des plans régionaux de gestion des incidents critiques, la formation sur le Système de commandement des interventions et d'autres plans et produits de gestion des urgences;
- Favoriser et coordonner l'état de préparation opérationnelle au sein des régions et coordonner le réseau des coordonnateurs de la gestion régionale des urgences;
- Assurer l'intégration complète des activités de gestion des urgences opérationnelles dans le Cadre intégré de gestion des urgences;
- Diriger les plans de continuité des activités opérationnelles, régionales et des points d'entrée et d'autres exercices.

**Gestion de la continuité des activités**

La gestion de la continuité des activités englobe l'élaboration et l'exécution en temps opportun des plans de continuité des activités, des activités connexes, des procédures et des ententes veillant à une interruption minimale ou nulle de l'accessibilité aux services et aux biens essentiels pour la population canadienne en cas d'évènements importants perturbateurs pour les activités de l'Agence.



Les activités sont les suivantes :

- diriger la mise en œuvre du processus de continuité des activités à l'intérieur du cadre de gestion des urgences et veiller à ce que des plans de continuité des activités (PCA) soient en place pour tous les services essentiels et les services de soutien essentiels;
- diriger l'analyse des répercussions sur les activités (ARA) afin d'évaluer l'incidence des évènements sur les services, les biens et les dépendances de l'Agence;
- coordonner la préparation des plans par la tenue d'exercices;
- fournir une surveillance et un contrôle stratégiques;
- assurer la liaison avec les organismes centraux et les autres ministères ainsi que la participation de ceux-ci dans le cadre des initiatives et des exigences au chapitre de la continuité des activités.

**Gestion de la continuité des TI**

La planification de la continuité des activités (PCA) comprend l'élaboration et l'exécution en temps opportun de plans, mesures, procédures et ententes veillant à une interruption minimale ou nulle de l'accessibilité aux services et aux biens essentiels en cas d'évènements importants perturbateurs pour les activités de l'Agence.

Les activités sont les suivantes :

- élaborer et mettre à jour le programme de continuité des TI;
- élaborer et mettre à jour le programme de reprise après sinistre;
- administrer et soutenir le logiciel PRREP (Planning, Response, Recovery, Emergency Preparedness);
- concevoir et mettre en œuvre des programmes de sensibilisation à la continuité des TI;
- élaborer et mettre en œuvre des programmes et des activités opérationnelles visant des interventions et une gestion efficaces des incidents de sécurité informatique, dont la coordination avec des organismes externes, au besoin;
- diriger les exercices sur la reprise des activités après un sinistre;
- contrôler et signaler les situations ayant des incidences sur les opérations de TI de l'ASFC;
- offrir un point central à l'ASFC, 24 heures sur 24, sept jours sur sept pour les interventions en cas de catastrophe par l'entremise du Centre d'intervention des technologies de l'information (CITI);
- fournir une évaluation continue des capacités de rétablissement gérées par le fournisseur de services externes, afin de garantir la satisfaction de toutes les exigences de l'ASFC;
- élaborer, tenir à jour et assurer le suivi des stratégies, des politiques, et des processus en lien avec la continuité des TI, ainsi que des cadres de gestion des risques, tout en assurant la conformité à la gestion de la sécurité des technologies de l'information et aux politiques, directives et normes de sécurité du gouvernement du Canada;
- diriger la mise en œuvre du programme de continuité des TI au sein du cadre de gestion des urgences et faire en sorte que des plans de continuité des TI et de rétablissement en cas de sinistre soient en place pour tous les services et systèmes de TI de première importance.

**Direction du Centre national des opérations frontalières, Direction générale des opérations**
**Section de gestion des urgences et Centre des opérations frontalières (COF)**



La *Section de gestion des urgences* fournit une surveillance du programme et une orientation quant aux mesures opérationnelles liées à la gestion des urgences dans les régions et maintient l'état de préparation opérationnelle.

Les activités sont les suivantes :

- assurer une gestion de programme en ce qui concerne les mesures opérationnelles liées à la gestion des urgences et aider les régions dans le cadre de l'établissement et de l'actualisation des plans, des produits, des exercices, etc. relatifs à la gestion des urgences dans les régions;
- promouvoir et coordonner l'état de préparation opérationnelle au sein des régions;
- veiller à la pleine intégration des activités opérationnelles de gestion des urgences dans le Cadre intégré de gestion des urgences;
- diriger les exercices opérationnels.

Centre des opérations frontalières (COF)

Le Centre des opérations frontalières (COF) est ouvert 24 heures sur 24, sept jours sur sept. Il s'agit d'un centre de communication et de coordination centralisé pour le signalement d'évènements et de problèmes qui touchent l'ASFC. Il contribue à fournir des interventions uniformes à l'échelle nationale et à établir un processus pour ce qui est de la notification et la gestion des événements importants et des urgences. Le BOC fournit du soutien opérationnel aux employés des régions au Canada et à l'étranger.

Les activités sont les suivantes :

- sensibiliser la haute direction aux événements, activités et questions à venir pouvant avoir une incidence sur l'exécution du mandat de l'Agence ou la perception de l'Agence par le public;
- agir comme point de contact principal pour les intervenants internes et externes et les bureaux de première responsabilité (BPR) pour faire face aux évènements importants;
- appuyer la planification de la continuité des activités de l'Agence;
- soutenir la gestion et l'intervention de l'ASFC grâce à la communication et au signalement cohérents des évènements, des problèmes et des incidents qui influent sur l'Agence.

**Santé et sécurité**

L'ASFC doit veiller à la santé et à la sécurité de ses employés et des visiteurs de ses installations. Dans le cadre du programme de sécurité de l'ASFC, cette responsabilité s'inscrit directement dans la protection des employés contre la violence au travail et d'autres exigences établies par la partie II du *Code canadien du travail* et d'autres instruments de politique du SCT. Bien que la responsabilité de la sécurité des employés dans ce contexte relève de l'ASM, la *Division de la santé et de la sécurité au travail* de la Direction des relations de travail et de la rémunération, Direction générale des ressources humaines, a la responsabilité de veiller à ce qu'un programme soit en place pour protéger la santé et la sécurité des employés dans le milieu de travail.

Les activités sont les suivantes :

- fournir un service de consultation et d'orientation à la direction de l'ASFC sur les questions relatives à la partie II du *Code canadien du travail* et aux directives du Conseil national mixte du SCT;







- élaborer la politique « Prévention de la violence en milieu de travail » et faire en sorte qu'elle soit passée en revue de manière régulière;
- élaborer un programme obligatoire relatif à la santé et à la sécurité au travail pour tous les employés et veiller à ce que l'ensemble du personnel bénéficie d'une formation adéquate sur ce programme;
- assumer le rôle de secrétariat pour le Comité d'orientation en matière de santé et de sécurité au travail;
- assurer la coordination avec la Direction de la sécurité et des normes professionnelles (DSNP) en ce qui touche les questions relatives à la protection des employés contre la violence au travail;
- assurer la liaison avec la DSNP pour ce qui est des procédures d'urgence et des exigences liées aux plans d'évacuation.

## 4. Surveillance et contrôle

La surveillance et le contrôle sont requis pour assurer le suivi des progrès réalisés et transmettre les résultats. La *Surveillance des programmes et évaluation des risques* permet de faire en sorte que la cohérence du programme de sécurité nationale soit appuyée par la surveillance accrue du rendement et la communication de données au moyen des rapports trimestriels destinés au Comité exécutif, et que la prestation des services de sécurité s'harmonise davantage aux priorités et aux exigences opérationnelles de l'Agence. Les activités englobent : le Rapport sur le rendement de l'Agence (RRA), la coordination du modèle de gestion fonctionnel (MGF) et la production de rapports connexes, la planification de la mesure du rendement et la présentation des rapports connexes.

Les activités sont les suivantes :

- mettre sur pied et tenir à jour un programme de surveillance pour appuyer les relations hiérarchiques fonctionnelles avec les directeurs régionaux de la sécurité, les gestionnaires régionaux de la sécurité et le personnel du programme de sécurité à l'AC;
- coordonner la production de rapports sur les activités liées à la mesure du rendement;
- élaborer une base de données exhaustive sur les tendances afin de surveiller, d'analyser et d'interpréter les tendances;
- élaborer une stratégie de surveillance liée aux principaux contrôles de sécurité et aux mesures recueillies et assurer une surveillance à cet égard;
- coordonner les normes de mesures de rendement pour les programmes de la Direction de la sécurité et des normes professionnelle.

## 5. Mesure et évaluation du rendement

On procède à des examens trimestriels afin d'évaluer l'efficacité du programme de sécurité de l'Agence, de vérifier si les buts, les objectifs stratégiques et les objectifs de contrôle précisés dans le plan ministériel de sécurité de l'Agence ont été atteints et si le plan est toujours pertinent pour les besoins de l'Agence et du gouvernement dans son ensemble.

De façon continue, on mesure le rendement pour veiller :





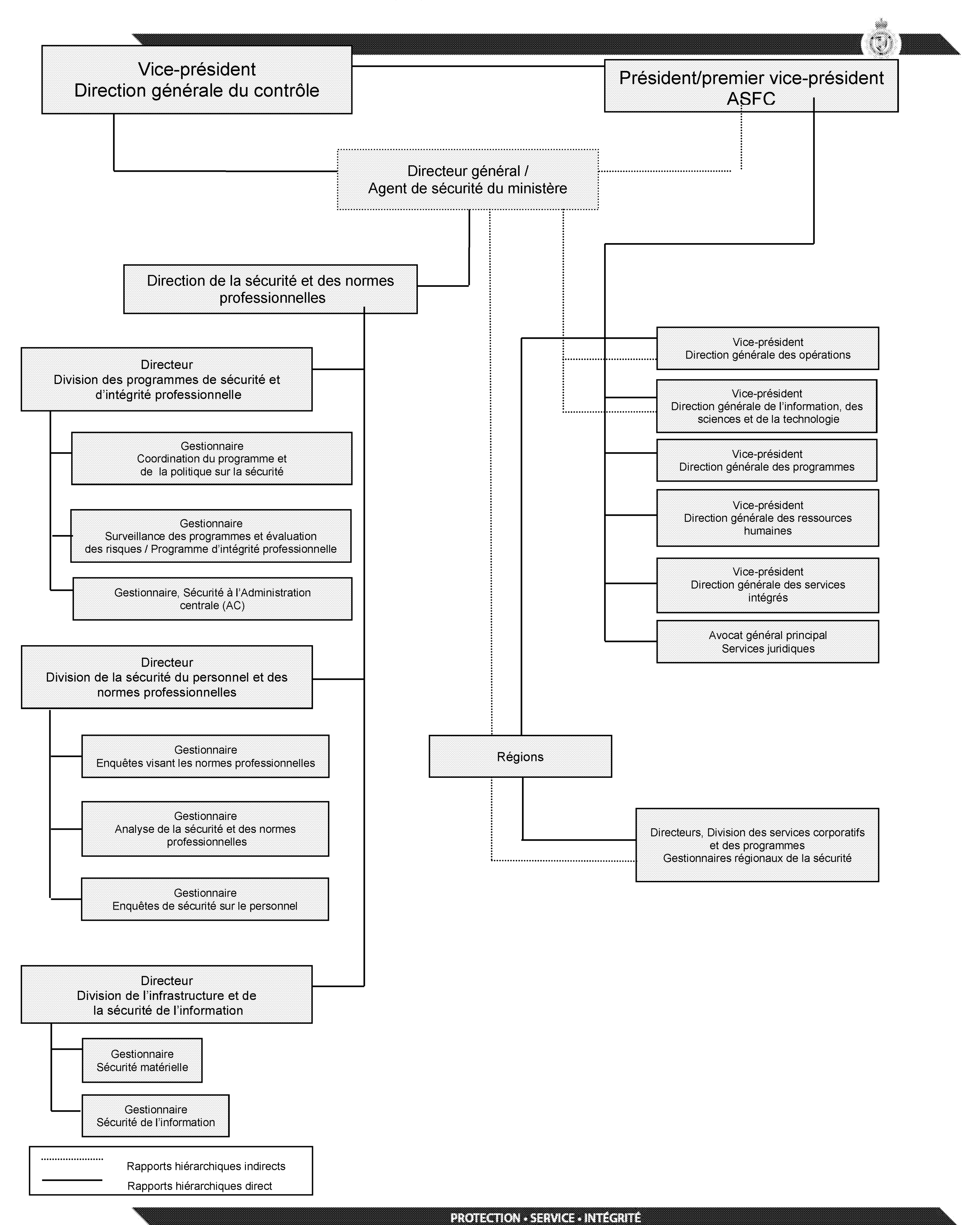
- à l'existence d'un programme d'assurance de la qualité qui vérifie si les contrôles de sécurité respectent les exigences en matière de sécurité de l'Agence, de la façon la plus efficiente et efficace qui soit;
- à l'atteinte et au maintien d'un niveau acceptable de risques résiduels.

L'ASFC a la responsabilité de faire des rapports périodiques au SCT sur l'état et l'avancement de la mise en œuvre de la PSG et sur les résultats de la mesure du rendement continue.

## 6. Soutien à l'échelle du gouvernement

L'ASFC offre son leadership, innove et contribue constamment au programme de sécurité à l'échelle du gouvernement par :

- la participation aux comités de sécurité du SMA et des DG présidés par le SCT;
- la participation aux divers groupes de travail dirigés par différents organismes centraux ;
- la participation aux réunions interministérielles des coordonnateurs de la sécurité des TI et des agents de sécurité ministériels présidées par le SCT, ainsi qu'au groupe de travail sur la cybersécurité.


Agence des services frontaliers du Canada
Canada Border Services Agency
Vice-président
Direction générale du contrôle
Président/premier vice-président
ASFC
Directeur général /
Agent de sécurité du ministère
Direction de la sécurité et des normes professionnelles
Directeur
Division des programmes de sécurité et d'intégrité professionnelle
Gestionnaire
Coordination du programme et de la politique sur la sécurité
Gestionnaire
Surveillance des programmes et évaluation des risques / Programme d'intégrité professionnelle
Gestionnaire, Sécurité à l'Administration centrale (AC)
Directeur
Division de la sécurité du personnel et des normes professionnelles
Gestionnaire
Enquêtes visant les normes professionnelles
Gestionnaire
Analyse de la sécurité et des normes professionnelles
Gestionnaire
Enquêtes de sécurité sur le personnel
Directeur
Division de l'infrastructure et de la sécurité de l'information
Gestionnaire
Sécurité matérielle
Gestionnaire
Sécurité de l'information
Vice-président
Direction générale des opérations
Vice-président
Direction générale de l'information, des sciences et de la technologie
Vice-président
Direction générale des programmes
Vice-président
Direction générale des ressources humaines
Vice-président
Direction générale des services intégrés
Avocat général principal
Services juridiques
Régions
Directeurs, Division des services corporatifs et des programmes
Gestionnaires régionaux de la sécurité
Rapports hiérarchiques indirects
Rapports hiérarchiques direct
PROTECTION • SERVICE • INTÉGRITÉ
Canada


Agence des services frontaliers du Canada    Canada Border Services Agency



# Annexe B – Structure de responsabilisation du programme de sécurité de l'ASFC

Le graphique ci-dessus démontre la Structure de responsabilisation du programme de sécurité de l'Agence des services frontaliers du Canada.

Le gestionnaire de la Sécurité matérielle et le gestionnaire de la Sécurité de l'information rendent compte directement au Directeur de la Division de l'infrastructure et de la sécurité de l'information.

Le gestionnaire des Enquêtes de sécurité sur le personnel, le gestionnaire de l'Analyse de la sécurité et des normes professionnelles et le gestionnaire des Enquêtes visant les normes professionnelles rendent compte directement au Directeur de la Division de la sécurité du personnel et des normes professionnelles.

Le gestionnaire de la Sécurité à l'Administration centrale (AC), le gestionnaire de la Surveillance des programmes et évaluation des risques/Programme d'intégrité professionnelle et le gestionnaire de la Coordination du programme et de la politique sur la sécurité rendent compte directement au Directeur de la Division des programmes de sécurité et d'intégrité professionnelle.

Le Directeur de la Division de l'infrastructure et de la sécurité de l'information, le Directeur de la Division de la sécurité du personnel et des normes professionnelles et le Directeur de la Division des programmes de sécurité et d'intégrité professionnelle rendent compte directement au Directeur général/Agent de sécurité du ministère de la Direction de la sécurité et des normes professionnelles.

Le Directeur général/Agent de sécurité du ministère rend compte directement au Vice-président de la Direction générale du contrôle et rend compte indirectement au Président/premier vice-président de l'Agence des services frontaliers du Canada.

Le Vice-président de la Direction générale du contrôle rend compte directement au Président/premier vice-président de l'Agence des services frontaliers du Canada.

Les Directeurs, Division des services corporatifs et des programmes ainsi que les gestionnaires régionaux de la sécurité rendent compte directement au Vice-président de la Direction générale des opérations.



Les Directeurs, Division des services corporatifs et des programmes ainsi que les gestionnaires régionaux de la sécurité rendent compte indirectement au Directeur général/Agent de sécurité du ministère.

L'Avocat général principal des Services juridiques, le Vice-président de la Direction générale des services intégrés, le Vice-président de la Direction générale des ressources humaines, le Vice-président de la Direction générale des programmes, le Vice-président de la Direction générale de l'information, des sciences et de la technologie et le Vice-président de la Direction générale des opérations rendent compte directement au Président/premier vice-président de l'Agence des services frontaliers du Canada.

Le Vice-président de la Direction générale de l'information, des sciences et de la technologie et le Vice-président de la Direction générale des opérations rendent compte indirectement au Directeur général/Agent de sécurité du ministère et le Président/premier vice-président de l'Agence des services frontaliers du Canada.



Annexe C – Mandat du Comité de gestion de la sécurité

# Comité de gestion de la sécurité

## Mandat

### 1. Position dans la structure de gouvernance

Le Comité de gestion de la sécurité (CGS) est un comité au niveau de la haute direction présidé par l'agent de sécurité du ministère (ASM), responsable de fournir des conseils relatifs à la gestion stratégique du Programme de sécurité de l'Agence au Comité de gestion de l'Agence (CGA) et au Comité exécutif, le cas échéant.

### 2. Mandat

Le mandat du CGS est de :

- établir une orientation stratégique pour la sécurité de l'ASFC;
- servir d'organisme de consultation pour les questions de sécurité en cours et émergeantes;
- établir une direction stratégique et fournir une orientation fonctionnelle et le soutien dans ce domaine au vice-président, Direction générale du contrôle;
- Soulever les questions litigieuses au Comité de gestion de l'Agence (CGA) pour une nouvelle délibération et décision (p. ex. les impacts liés à la sécurité concernant l'élaboration de programmes et de politiques);
- présenter au Comité exécutif (CE) et ou au Président, les questions de sécurité qui restent sous la seule responsabilité du Président conformément à la délégation de pouvoir à l'agent de sécurité du ministère (ASM) et la Politique sur la sécurité du gouvernement.

### 3. Membres

Le membership est composé de représentants des directions générales à l'administration centrale et des régions:

Président



- Agent de sécurité du ministère (ASM) et Directeur général, Direction de la sécurité et des normes professionnelles, Direction générale du contrôle

Président suppléant

- Directeur général, Direction du centre national des opérations frontalières, Direction générale des opérations

Membres

- Directeur général, Direction des services d'entreprise, Direction générale de l'information, des sciences et de la technologie
- Directeur général, Direction de l'évaluation stratégique des risques et Modernisation, Direction générale des programmes
- Directeur général, Direction des relations de travail et de la rémunération, Direction générale des ressources humaines
- Directeur général, Direction de l'infrastructure et des opérations environnementales, Direction générale du contrôle
- Directeur principal, Division des services consultatifs des communications, Direction des communications, Direction générale des services intégrés
- Directeur, Division des programmes de sécurité et d'intégrité professionnelle, Direction générale du contrôle
- Directeur, Division de la sécurité du personnel et des normes professionnelles, Direction générale du contrôle
- Directeur, Division de la sécurité de l'information et de l'infrastructure, Direction générale du contrôle
- Gestionnaire, Section de la gestion des urgences, Direction générale des opérations
- Directeur, Division de la sécurité et de la continuité de la TI, Direction générale de l'information, des sciences et de la technologie
- Directeur général régional (région de l'Atlantique)
- Directeur régional, Division des services intégrés et aux programmes, responsable de la sécurité (région de l'Atlantique)
- Directeur général régional (région du Québec)
- Directeur régional, Division des services intégrés et aux programmes, responsable de la sécurité (région du Québec)
- Directeur général régional (région du nord de l'Ontario)



- Directeur régional, Division des services intégrés et aux programmes, responsable de la sécurité (région du nord de l'Ontario)
- Directeur général régional (région du Grand Toronto)
- Directeur régional, Division des services intégrés et aux programmes, responsable de la sécurité (région du Grand Toronto)
- Directeur général régional (région du sud de l'Ontario)
- Directeur régional, Division des services intégrés et aux programmes, responsable de la sécurité (région du sud de l'Ontario)
- Directeur général régional (région des prairies)
- Directeur régional, Division des services intégrés et aux programmes, responsable de la sécurité (région des prairies)
- Directeur général régional (région du Pacifique)
- Directeur régional, Division des services intégrés et aux programmes, responsable de la sécurité (région du Pacifique)

**Des experts en la matière peuvent être invités pour des points spécifiques sujets selon les besoins, à la discrétion du Président.

Secrétariat

L'appui du secrétariat sera assuré par le Conseiller en sécurité, Section de la coordination des politiques et des programmes, Direction générale du contrôle.

Le secrétariat est responsable de :

- envoyer les invitations à tous les membres leur demandant de contribuer à l'ordre du jour, trois (3) semaines avant chaque réunion.
- rédiger les ordres du jour (actuels et à venir) et obtenir l'approbation du Président;
- fournir les ordres du jour finaux et le matériel de réunion à tous les membres quatre (4) jours avant chaque réunion;
- préparer le Compte rendu des décisions et des mesures principales à prendre après chaque réunion pour l'examen et l'approbation du Président avant de l'envoyer à tous les membres pour leur examen et commentaires en dans des quatre (4) jours après la tenue de la réunion;
- Faire des suivis sur les actions clés et faire rapport au président.

## 4. Remplaçants aux réunions

Les membres du CGS peuvent nommer un (1) remplaçant prédéterminé au niveau directeur pour assister aux réunions lorsque le membre lui-même ne peut assister.

**5. Quorum**

Un minimum of huit (8) membres en plus du Président ou Président suppléant est nécessaire pour que la réunion soit reconnue comme une réunion autorisée à moins d'indication contraire de la part du Président.

Si le président n'est pas disponible pour assister une la réunion, le président-suppléant présidera la réunion.

**6. Autorité**

Le président du CGS a le pouvoir de :

- diriger l'orientation stratégique générale du comité;
- diriger l'orientation stratégique annuelle du comité;
- d'approuver les ordres du jour et de demander que des sujets soient présentés à une date précise;
- Le président conserve le pouvoir de décision sur les questions soumises au comité, toutefois, le président doit chercher à établir un consensus entre les membres dans l'accomplissement de son devoir.

En cas de besoin, le comité peut former des sous-comités, présidés par des membres du comité permanent, qui pourraient inclure d'autres participants afin d'aider à la réalisation du mandat du comité.

**7. Tâches et responsabilités**

Les tâches et responsabilités du CGS comprennent :

La sécurité

Le CGS veillera à la protection et à la sécurité des employés, la confidentialité, l'intégrité et la disponibilité de tous les biens de l'ASFC, y compris l'information, et assurera la prestation des programmes de base de l'ASFC liés à la sécurité. Il veillera à :

- fournir des conseils et direction sur des questions liées à tous les éléments de sécurité tels : le personnel, l'information, les biens matériels, les biens contrôlés et la technologie de l'information;
- assurer de former des liens appropriés et de consulter avec les représentants touchés par les questions de gestion de la sécurité;
- assurer que les programmes de sensibilisation à la sécurité soient développés pour les gestionnaires et les employés concernant leur rôles et responsabilités liés à la gestion de la sécurité;







- assurer que les politiques de sécurité, procédures, normes, et lignes directrices sur la prestation des programmes soient mises à jour en réponse aux changements (p. ex., les exigences du Secrétariat du conseil du trésor, les leçons apprises etc.) et communiqués aux employés;
- fournir la direction et l'endossement des politiques de sécurité (y compris les instruments de politique telles les directives, les normes et leurs annexes qui peuvent avoir un impact significatif sur les programmes), programmes et priorités;
- examiner et endosser les activités de gestion de la sécurité en relation avec le plan stratégique des activités associées à la sécurité;
- examiner les activités de gestion du rendement ainsi que les activités pour les programmes clés de sécurité;
- examiner et approuver les priorités du programme de sécurité;
- assurer un programme de surveillance et de rapport régulier en matière de sécurité au sein de chaque direction générale et des régions permettant la consultation et la résolution de problèmes au cours des réunions du CGS et à identifier les questions litigieuses qui doivent être apportées à l'attention du CGE pour une nouvelle délibération et décision ;
- développer des sous-comités du CGS pour adresser des questions spécifiques (au besoin);
- collaborer et résoudre des questions qui touchent les domaines de la sécurité, de la gestion des urgences et de la continuité des opérations communiqués par le Groupe de travail de la sécurité, les opérations et la continuité, lors des réunions du CGS.

## 8. Fréquence et durée

Les réunions du CGS auront lieu tous les deux (2) mois pour une période de deux (2) heures et alterneront avec les réunions du Groupe de travail de la sécurité, les opérations et la continuité qui auront lieu à tous les deux (2) mois également.

Le rééchelonnement des réunions du comité sera effectué par exception seulement.

Le président a le droit de convoquer des réunions ad hoc lorsque les circonstances l'exigent.

## 9. Gestion du rendement

Le président du CGS doit examiner les progrès du comité contre le plan stratégique sur une base trimestrielle. Cela assurera que les travaux du







comité sont correctement alignés avec et supportent la réalisation des objectifs stratégiques de l'Agence.

Révisé le 12 avril 2014

Canada Border Services Agency / Agence des services frontaliers du Canada



# Directive on CBSA Personnel Security Screening

PROTECTION • SERVICE • INTEGRITY



## CBSA Personnel Security Screening Directive

### 1. Effective Date

1.1. This directive takes effect on January 6, 2015.

### 2. Application

2.1. This directive applies to:

- All individuals who will have access to Canada Border Services Agency (CBSA) information and assets; and
- All applicants to and employees (permanent, term, casual, part-time) of the CBSA, contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students.

### 3. Context

The Government of Canada's Policy on Government Security (PGS) requires the CBSA to ensure that all individuals who will have access to government information and assets are security screened at the appropriate level before the commencement of their duties and are treated in a fair and unbiased manner. This directive describes how the CBSA will manage Personnel Security in accordance with the PGS.

Security begins by establishing trust in interactions between government and Canadians and within government. Within government, there is a need to ensure that those having access to government information, assets and services are trustworthy, reliable and loyal. The CBSA's Personnel Security Program has been established to support these requirements.

The Personnel Security Program limits access to information and assets to those individuals with a need to know. It ensures that an individual is appropriately screened based on the information and access required for the performance of his or her job. Effective Personnel Security management enables the CBSA:

- To ensure that individuals with access to government information/assets and/or privileged access to critical systems are reliable and trustworthy;
- To ensure the individual's loyalty to Canada in order to protect itself from foreign intelligence gathering and terrorism; and
- To prevent malicious activity and unauthorized disclosure of protected and classified information or damage affected on critical systems by a disaffected individual in a position of trust.

In recognition of the CBSA's role in law enforcement, national security and public safety and the demonstrated risk exposure to incidents of corruption, fraud and criminal interference, the Agency





received Treasury Board approval to implement additional Personnel Security screening tools to augment the baseline screening requirements.

**4. Definitions**

Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

**5. Policy Statement**

**5.1. Objective**

The objective of this directive is to ensure that the CBSA provides the appropriate access to Government of Canada (GoC) information and assets to personnel who have been deemed trustworthy and loyal in accordance with the Policy on Government Security (PGS).

**5.2. Expected Results**

- Compliance with the PGS;
- Employees understand their responsibilities regarding the security of Government information and assets;
- Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;
- Interoperability and information exchange with other GoC Personnel Security Departments and Agencies;
- Mechanisms and resources are in place to ensure effective and efficient management of Personnel Security at the CBSA;
- Individuals with access to Agency information and assets have integrity, are reliable, honest and trustworthy;
- The vulnerability to influence by criminal elements is reduced;
- The potential security risks to sensitive information and assets are minimized; and
- The protection of program integrity.

**6. Roles and Responsibilities**

**6.1. President**

The President of the CBSA is responsible for effectively managing security activities within the CBSA and contributing to effective government-wide security management. The President is responsible for:

- Ensuring the CBSA's compliance to the PGS and other related policy instruments and legislation;

- Approving the CBSA's Departmental Security Plan and establishing a security program for the coordination and management of overall security activities, including Personnel Security;
- Appointing a Departmental Security Officer to manage the departmental security program;
- Ensuring that managers at all levels integrate Personnel Security requirements into plans, programs, activities and services;
- Denying, suspending or revoking a Reliability Status in the case of just cause;
- Denying, suspending or revoking a Security Clearance in the case of just cause; and
- Ensuring that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence, they are investigated, acted upon and reported to the appropriate authorities.

### 6.2. Departmental Security Officer (DSO)

The Departmental Security Officer (DSO) is responsible for the management of CBSA's Security Program and has the following responsibilities with regard to Personnel Security:

- Developing, implementing, monitoring and maintaining a Departmental Security Plan which incorporates Personnel Security;
- Ensuring a coordinated approach to all aspects of CBSA Security: Personnel Security, IM, COMSEC, Contract and Physical Security;
- Ensuring that accountabilities, delegations, reporting relationships, and roles and responsibilities of CBSA employees with security responsibilities are defined, documented and communicated to relevant persons;
- Granting a Reliability Status and Security Clearance;
- Delegating the granting of a Reliability Status and Security Clearance by the DSO;
- Giving advice and making recommendations to the President in cases of denial, suspension or revocation of a Security Clearance; and
- Where just cause exists:
  - Denying, revoking or suspending a Reliability Status and informing the manager or Director.

### 6.3. Personnel Security Screening Section

The Personnel Security Screening Section (PSSS) is responsible for the coordination of all functions related to the technical and operational aspects of Personnel Security, specifically:

- Ensuring that all individuals who require access to Protected/Classified information or/and assets or/and privileged access to critical systems, have been granted the required CBSA approved Security level **prior** to the start of any assignment, appointment or secondment as a Reliability status or a Security Clearance is a condition of employment at the CBSA.
  - Reliability Status is required if access to Protected (A, B or C) information is a requirement of the work duties.

- A Secret Security Clearance is required if access to Classified information is a requirement of the work duties. It is also required when privileged access to critical systems is needed to perform work duties.
- Top Secret clearance is required if access to Classified information is a requirement of the work duties and there is a need to know to access information classified as Top Secret.

- Maintaining a functional or direct reporting relationship with the DSO to ensure departmental security activities are coordinated and integrated;
- Selecting, implementing and maintaining security controls related to the Personnel Security;
- Determining the security requirements of each position based on the sensitivity of the information, assets and privileged access to critical systems to which the incumbent has access;
- Advising managers and/or Human Resources (HR) of the status of the security assessment;
- Processing requests for personnel security screenings, including criminal record name checks, credit checks, verification of databases with Customs and Immigration information, Law Enforcement Record Checks, conducting integrity interviews, and conducting loyalty assessments ;
- Advising HR, Regional Security or HQ Security in writing of the candidate's personnel security screening results;
- Ensuring that all employees / contractors have received the official briefing by the employee's manager and have signed the Security Screening Certificate and Briefing Form;
- Maintaining employee personnel security screening files;
- Ensuring that Reliability Status and Security Clearances are updated, in accordance with the Security requirements of the position. The Security Officer will update:
  - a Reliability Status: every 10 years
  - a Secret clearance: every 10 years
  - a Top Secret clearance: every 5 years
- Conducting an update to the security screening of any employee who has been away from the workplace for over 1 year; and
- Performing reviews of screenings for cause and conducting investigations when required.

### 6.4. Regional/Headquarters Security Manager

Regional and Headquarters Security Managers are responsible for:

- Providing advice and guidance regarding the security screening process;
- Reviewing the completed personnel security screening forms for accuracy prior to forwarding it to the PSSS; and
- Ensuring that integrity interviews are conducted when required by PSSS.

### 6.5. Human Resources

Human Resources are responsible for:

- Verifying the following information for new employees:
  - Personal data (i.e. date of birth, address)
  - Education / professional qualifications
  - Employment history
  - Personal Character
- Initiating the Personnel Security Screening process; and
- Ensuring that no employee is hired/appointed/acting in a position without being security screened and granted his or her required CBSA Reliability Status or Security Clearance by the DSO.

**6.6. CBSA Managers**

Managers are responsible for:

Managers are responsible for ensuring an appropriate level of security for their programs and services. In designing programs and services, managers will work with departmental security specialists to effectively manage risk. Managers will be supported and assisted by the PSSS in order to fulfill the following responsibilities:

- Ensuring that security requirements are integrated into business planning, programs, services and other management activities;
- Ensuring employees apply effective security practices;
- Identifying the sensitivity of the information, assets and privileged access to critical systems for each position of their unit and informing the CBSA PSSS to obtain the proper Security requirement for the position;
- Ensuring that no individual is hired/appointed/acting or commences any work in a position without being screened and granted his or her required CBSA approved Security Level by the PSSS, including acting assignments;
- Controlling access to protected/classified information and assets to persons who have acquired the proper Security Clearance and who have a "need-to-know"; need-to-know means the need for someone to access and know information in order to perform his or her duties.
- When contracts are required, identifying any security requirements and ensuring that no temporary help, contractor or consultant is hired or commences any work without being screened and has been granted the appropriate CBSA approved security level as required in the contract or agreement;
- Reporting adverse information to the Security and Professional Standards Directorate (SPSD);
- Ensuring that a Security Briefing is provided to every employee upon hire; and
- Ensuring that employees take the Online Security Awareness Module within two weeks of joining the CBSA and repeating the module every two years thereafter.

**6.7. Employees**

Employees are responsible for:

- Safeguarding information and assets under their control whether working on CBSA premises or off-site;
- Applying security controls related to their area of responsibility to ensure that security requirements are part of their day-to-day processes, practices and program delivery;
- Reporting security incidents through the appropriate channels; and
- Informing their manager of any issues affecting their Reliability Status or Security Clearance:
    - Arrest or Criminal conviction;
    - Bankruptcy;
    - Single/cohabitating/marriage/divorce; and/or
    - If approached by someone criminal, a representative of a foreign government, a fringe interest group or a foreign national who is seeking information about CBSA or the activities of CBSA, which would compromise the national interest, or the integrity of the Agency.

**7. Consequences**

CBSA employees are held to high standards based on the nature of the work they do. There is a requirement for CBSA employees to have honesty, integrity and trustworthiness – the HIT factor. CBSA employees who are found to have breached the HIT factor, CBSA Code of Conduct, the Policy on Government Security, the Values and Ethics Code or any other applicable CBSA or Government of Canada policies, standards or legislation, will be subject to disciplinary measures based on the seriousness of the misconduct and in accordance with the CBSA Discipline Policy. In some cases this may mean a review and possibly a revocation of the CBSA Reliability Status.

**8. References**

This directive is issued under section 7 of the Financial Administration Act and should be read in conjunction with:

- CBSA Personnel Security Screening Standard
- Security Requirements for CBSA Contracts  Standard Operating Procedures for Security Requirement Checklist (SRCL)
- Policy on Government Security
- Directive on Identity Management
- Directive on Departmental Security Management
- Standard on Security Screening
- Operational Security Standard: Management of Information Technology Security (MITS)
- CBSA Code of Conduct
- Values and Ethics Code for the Public Sector
- Criminal Code of Canada

**9. Enquiries**

For more information, please contact:
Security and Professional Standards Directorate
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive concernant les enquêtes de sécurité sur le personnel de l'ASFC

PROTECTION • SERVICE • INTÉGRITÉ

Canada





## Directive concernant les enquêtes de sécurité sur le personnel de l'ASFC

### 1. Date d'entrée en vigueur

1.1. Cette directive entre en vigueur le 6 janvier 2015.

### 2. Application

2.1. Cette directive s'applique à :

- toutes les personnes qui auront accès aux renseignements et aux biens de l'Agence des services frontaliers du Canada (ASFC);
- tous les postulants à l'ASFC et aux employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), au personnel contractuel et au personnel d'agences privées, ainsi qu'aux personnes en détachement ou en affectation à l'ASFC, y compris les étudiants.

### 3. Contexte

La Politique sur la sécurité du gouvernement (PSG) exige de l'ASFC de s'assurer que toutes les personnes qui auront accès aux renseignements et aux biens du gouvernement font l'objet d'enquêtes de sécurité au niveau approprié avant le début de leurs fonctions et soient traitées d'une manière juste et impartiale. Cette directive décrit la façon dont l'ASFC devra gérer la sécurité du personnel conformément à la Politique sur la sécurité du gouvernement.

La sécurité commence par l'établissement d'une confiance dans les interactions entre le gouvernement et les Canadiens ainsi que dans celles prenant place au sein du gouvernement lui-même. Au sein du gouvernement, il est nécessaire de veiller à ce que ceux qui ont accès aux renseignements, aux biens et aux services gouvernementaux soient dignes de confiance, fiables et loyaux. Le Programme de sécurité du personnel de l'ASFC a été créé pour répondre à ces exigences.

Le Programme de sécurité du personnel limite l'accès aux renseignements et biens aux personnes ayant un besoin de connaître. Il permet de s'assurer qu'une personne fait l'objet d'une enquête de sécurité au niveau approprié en fonction des renseignements et de l'accès dont elle a besoin pour s'acquitter de ses fonctions. Une gestion efficace de la sécurité du personnel permet à l'ASFC :

- de veiller à ce que les personnes ayant accès aux renseignements et biens et/ou ayant un accès privilégié aux systèmes essentiels soient fiables et dignes de confiance;
- d'assurer la loyauté des employés envers le Canada afin de se protéger contre les services de renseignements étrangers et le terrorisme;
- de prévenir tout acte malveillant et toute divulgation non autorisée de renseignements protégés et classifiés ainsi que tout dommage à des systèmes essentiels causés par le mécontentement d'une personne occupant un poste de confiance.









En reconnaissance du rôle de l'ASFC en matière d'exécution de la loi, de sécurité nationale et de sécurité publique ainsi que de l'exposition démontrée au risque d'incidents de corruption, de fraude et d'ingérence criminelle, l'Agence a reçu l'approbation, de la part du Conseil du Trésor, de mettre en œuvre des outils supplémentaires d'enquêtes de sécurité sur le personnel visant à accroître les exigences de base en matière de sécurité.

**4. Définitions**

Des définitions précises provenant de sources qui font autorité se trouvent à au Lexique de la terminologie en sécurité.

**5. Énoncé de la politique**

**5.1. Objectif**

L'objectif de la présente directive est de s'assurer que l'ASFC fournit au personnel qui a été jugé digne de confiance et loyal l'accès approprié aux renseignements et aux biens du gouvernement du Canada, conformément à la Politique sur la sécurité du gouvernement.

**5.2. Résultats attendus**

- l'ASFC se conforme à la Politique sur la sécurité du gouvernement.
- les employés comprennent leurs responsabilités en ce qui concerne la sécurité des renseignements et des biens du gouvernement.
- les renseignements, les biens et les services ne sont pas compromis et les employés sont protégés contre la violence en milieu de travail.
- l'interopérabilité et l'échange d'informations avec d'autres ministères et organismes du gouvernement du Canada responsables de la sécurité du personnel.
- des mécanismes et des ressources sont en place afin d'assurer une gestion efficace et efficiente de la sécurité du personnel à l'ASFC.
- les personnes ayant accès aux renseignements et aux biens de l'Agence sont intègres, fiables, honnêtes et dignes de confiance.
- la réduction de la vulnérabilité à l'influence des éléments criminels.
- les risques potentiels pour la sécurité des renseignements et des biens de nature délicate sont réduits au minimum.
- la protection de l'intégrité du programme.

**6. Rôles et responsabilités**

**6.1. Président**





Le président de l'ASFC est responsable de la gestion efficace des activités de sécurité au sein de l'ASFC et de la contribution à la gestion efficace de la sécurité à l'échelle du gouvernement. Il a les responsabilités suivantes :

- assurer le respect par l'ASFC de la Politique sur la sécurité du gouvernement et d'autres instruments de politique et lois connexes;
- approuver le Plan de sécurité ministérielle de l'ASFC et établir un programme de sécurité pour assurer la coordination et la gestion des activités globales de sécurité, y compris la sécurité du personnel;
- nommer un agent de sécurité du ministère chargé de la gestion du programme de sécurité;
- s'assurer que les gestionnaires à tous les niveaux intègrent les exigences en matière de sécurité du personnel dans les plans, les programmes, les activités et les services;
- refuser, suspendre ou révoquer une cote de fiabilité pour motif valable;
- refuser, suspendre ou révoquer une cote de sécurité pour motif valable;
- veiller à ce que les enjeux importants concernant le respect de la politique, les allégations d'inconduite, les activités criminelles présumées, les incidents de sécurité ou de violence en milieu de travail fassent l'objet d'enquêtes et de mesures de suivi et qu'ils soient signalés aux autorités compétentes.

### 6.2. Agent de sécurité du ministère (ASM)

L'agent de sécurité du ministère (ASM) est responsable de la gestion du Programme de sécurité de l'ASFC et a les responsabilités suivantes en ce qui concerne la sécurité du personnel :

- élaborer, mettre en œuvre, surveiller et tenir à jour un Plan de sécurité ministérielle qui intègre la sécurité du personnel;
- assurer une approche coordonnée de tous les aspects de la sécurité à l'ASFC : sécurité du personnel, GI, COMSEC, sécurité matérielle et des contrats;
- veiller à ce que les cadres de responsabilisation, les délégations, les rapports hiérarchiques, les rôles et les responsabilités des employés de l'ASFC qui ont des responsabilités en matière de sécurité soient définis, documentés et communiqués aux personnes concernées;
- accorder une cote de fiabilité et une cote de sécurité
- déléguer l'attribution de la cote de fiabilité et de sécurité par l'ASM
- donner des conseils et faire des recommandations au président en cas de refus, de suspension ou de révocation d'une cote de sécurité;
- en cas de motif valable :
    - refuser, retirer ou suspendre une cote de fiabilité et en informer le gestionnaire ou le directeur,

### 6.3. Section des enquêtes de sécurité sur le personnel

La Section des enquêtes de sécurité sur le personnel (SESP) est responsable de la coordination de toutes les fonctions liées aux aspects techniques et opérationnels de la sécurité du personnel, en particulier :





- veiller à ce que toutes les personnes qui doivent avoir accès aux renseignements et/ou aux biens protégés ou classifiés et/ou un accès privilégié aux systèmes essentiels aient obtenu la cote de sécurité au niveau requis approuvé par l'ASFC **avant** le début d'une affectation, d'une nomination ou d'un détachement. Une cote de fiabilité ou une cote de sécurité constituent une condition d'emploi à l'ASFC;
    - La cote de fiabilité est nécessaire si l'accès aux renseignements protégés (A, B ou C) est nécessaire pour l'exercice des fonctions.
    - Une cote de sécurité de niveau secret est nécessaire si l'accès aux renseignements classifiés est une exigence liée aux fonctions du poste. Elle est également nécessaire lorsque l'accès privilégié aux systèmes essentiels est nécessaire pour s'acquitter de ses tâches.
    - Une cote de sécurité très secrète est nécessaire si l'accès aux renseignements classifiés est une exigence liée aux fonctions du poste et s'il y a un « besoin de connaître » pour avoir accès aux renseignements classifiés très secret.

- maintenir une relation fonctionnelle ou de rapport direct avec l'ASM pour assurer la coordination et l'intégration des activités de sécurité ministérielle;
- sélectionner, mettre en œuvre et tenir à jour des contrôles de sécurité liés à la sécurité du personnel;
- déterminer les exigences en matière de sécurité de chaque poste en fonction de la nature délicate des renseignements, des biens et de l'accès privilégié aux systèmes essentiels auxquels l'employé a accès;
- informer les gestionnaires et/ou les Ressources humaines (RH) sur l'état de l'évaluation de la sécurité;
- traiter des demandes d'enquêtes de sécurité sur le personnel, y compris la vérification de l'existence d'un dossier judiciaire, la vérification du crédit, la vérification des bases de données comportant des renseignements sur les douanes et l'immigration, la vérification de dossiers policiers, mener des entrevues d'intégrité et mener des évaluations de la loyauté;
- informer les RH, le bureau régional de la sécurité ou la Sécurité à l'AC par écrit des résultats des enquêtes de sécurité sur le personnel du candidat;
- veiller à ce que tous les employés/entrepreneurs ont reçu la séance d'information officielle sur la sécurité par le gestionnaire de l'employé et qu'ils ont signé le Certificat d'enquête de sécurité et profil de sécurité;
- tenir à jour les dossiers d'enquête de sécurité sur le personnel des employés;
- veiller à ce que la cote de fiabilité et la cote de sécurité soient mises à jour avant leur expiration, en conformité avec les exigences en matière de sécurité liées au poste. L'agent de sécurité mettra à jour :
    - une cote de fiabilité : tous les 10 ans
    - une cote sécurité de niveau secret : tous les 10 ans
    - une cote sécurité de niveau très secret : tous les 5 ans
- faire une mise à jour de l'enquête de sécurité sur le personnel de tout employé absent du lieu de travail pendant plus d'un an;
- réviser les enquêtes de sécurité pour motif valable et mener des investigations lorsque c'est nécessaire.





### 6.4. Gestionnaires régionaux de la sécurité et gestionnaires de la sécurité de l'Administration centrale

Les gestionnaires régionaux de la sécurité et gestionnaires de la sécurité de l'Administration centrale ont les responsabilités suivantes :

- fournir des conseils et une orientation concernant le processus d'enquête de sécurité;
- examiner l'exactitude des formulaires d'enquête de sécurité sur le personnel remplis avant de les transmettre à la Section des enquêtes de sécurité sur le personnel;
- S'assurer que les entrevues d'intégrité soit menés lorsque requis par SESP.

### 6.5. Ressources humaines

Les Ressources humaines ont les responsabilités suivantes :

- vérifier les informations suivantes pour les nouveaux employés :
  - les données personnelles (par exemple la date de naissance, l'adresse)
  - le niveau d'études/les qualifications professionnelles
  - les antécédents professionnels
  - les traits de caractère personnels
- amorcer le processus d'enquête de sécurité sur le personnel;
- s'assurer qu'aucun employé n'est embauché/nommé/intérimaire sans que l'ASM ait fait une enquête de sécurité sur lui et lui a attribué la cote de fiabilité ou la cote de sécurité requise.

### 6.6. Gestionnaires de l'ASFC

Les gestionnaires ont les responsabilités suivantes :

Les gestionnaires doivent s'assurer que les programmes et services dont ils sont responsables sont dotés d'un niveau de sécurité approprié. Lors de la conception de programmes et de services, les gestionnaires doivent collaborer avec les spécialistes de la sécurité ministérielle afin de gérer efficacement les risques. Les gestionnaires seront appuyés et aidés par la Section des enquêtes de sécurité sur le personnel afin de s'acquitter des responsabilités suivantes :

- veiller à ce que les exigences en matière de sécurité soient intégrées à la planification des activités, aux programmes, aux services et aux autres activités de gestion;
- s'assurer que les employés appliquent les pratiques de sécurité efficaces;
- déterminer, pour chaque poste de leur unité, si l'accès à des renseignements et des biens de nature délicate ou un accès privilégié aux systèmes essentiels est nécessaire et en informer la Section des enquêtes de sécurité sur le personnel de l'ASFC afin d'obtenir le niveau de sécurité approprié pour le poste visé;





- s'assurer qu'aucun employé n'est embauché/nommé/intérimaire ou ne commence à travailler sans que la Section des enquêtes de sécurité sur le personnel ait fait une enquête de sécurité sur lui et lui a attribué la cote de sécurité requise approuvée par l'ASFC, y compris pour les affectations intérimaires;
- veiller à ce que l'accès aux renseignements et aux biens protégés ou classifiés soit permis uniquement aux personnes qui ont obtenu la cote de sécurité appropriée et qui ont « besoin de connaître »; le besoin de connaître est le besoin pour une personne d'accéder à des renseignements et de les connaître pour accomplir les tâches qui lui incombent;
- lorsque des contrats sont nécessaires, préciser les exigences en matière de sécurité et veiller à ce qu'aucun employé temporaire, entrepreneur ou consultant ne soit embauché ou ne commence à travailler sans avoir fait l'objet d'une enquête de sécurité et avoir obtenu la cote de sécurité appropriée approuvée par l'ASFC, conformément aux exigences du contrat ou de l'accord;
- signaler des renseignements défavorables à la Direction de la sécurité et des normes professionnelles;
- s'assurer qu'une séance d'information sur la sécurité est donnée à tous les employés à l'embauche;
- s'assurer que les employés suivent le Module en ligne de sensibilisation à la sécurité dans les deux semaines suivant leur arrivée à l'ASFC et qu'ils le suivent à nouveau tous les deux ans par la suite.

### 6.7. Employés

Les employées ont les responsabilités suivantes :

- protéger les renseignements et les biens dont ils ont la responsabilité, qu'ils travaillent dans les locaux de l'ASFC ou à l'extérieur;
- appliquer des mesures de contrôles de sécurité liées à leur domaine de responsabilité pour faire en sorte que les exigences de sécurité soient intégrées aux processus, aux pratiques et à l'exécution des programmes au quotidien;
- signaler les incidents de sécurité par les voies appropriées;
- informer leur gestionnaire de toute situation ayant une incidence sur leur cote de fiabilité ou de sécurité, telle que :
  - arrestation ou condamnation;
  - faillite;
  - célibat/cohabitation/mariage/divorce;
  - si abordé par une personne criminelle, un représentant d'un gouvernement étranger, un groupe d'intérêt marginal ou un ressortissant étranger qui désire obtenir des informations au sujet de l'ASFC ou des activités de l'ASFC, ce qui risquerait de mettre en péril l'intérêt national ou l'intégrité de l'Agence.

## 7. Conséquences

Les employés de l'ASFC sont tenus de respecter des normes élevées en raison de la nature du travail qu'ils font. Ils doivent faire preuve d'honnêteté, d'intégrité et de fiabilité – « le facteur HIF ». Les





employés de l'ASFC ayant violé les principes du « facteur HIF », le Code de conduite de l'ASFC , la Politique sur la sécurité du gouvernement ou le Code de valeurs et d'éthique, ou d'autres politiques, normes ou lois applicables de l'ASFC ou du gouvernement du Canada, feront l'objet de mesures disciplinaires selon la gravité de l'inconduite, conformément à la Politique en matière de discipline de l'ASFC. Dans certains cas, il peut s'agir d'une révision et peut-être d'une révocation de la cote de fiabilité de l'ASFC.

**8. Références**

La présente directive est émise en vertu de l'article 7 de la *Loi sur la gestion des finances publiques* et doit être lue conjointement avec :

- Norme d'enquêtes de sécurité sur le personnel de l'ASFC
- Procédures normales d'exploitation concernant la liste de vérifications des exigences relatives à la sécurité
- Politique sur la sécurité du gouvernement
- Directive sur la gestion de l'identité
- Directive sur la gestion de la sécurité ministérielle
- Norme sur le filtrage de sécurité
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)
- Code de conduite de l'ASFC
- Code criminel du Canada

**9. Demandes de renseignements**

Pour plus d'informations, veuillez-vous adresser à :
Direction de la sécurité et des normes professionnelles
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for CBSA Personnel Security Screening

PROTECTION • SERVICE • INTEGRITY



Canada Border Services Agency | Agence des services frontaliers du Canada



## Purpose

The purpose of this Standard is to ensure that in accordance with the Policy on Government Security (PGS), the Canada Border Services Agency (CBSA) security screens all individuals with access to government information and assets at the appropriate level before the commencement of their duties. The CBSA conducts its personnel security screening checks in accordance with the PGS - Personnel Security Standard, and additionally, conducts CBSA specific background checks at the Reliability Status level, which have been approved by the Treasury Board.

## Effective Date

This Standard takes effect on January 6, 2015.

## Application

The standard applies to:

- All individuals who will have access to Canada Border Services Agency (CBSA) information and assets; and
- All applicants to and employees (permanent, term, casual, part-time) of the CBSA, contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students.

## Context

Personnel Security Screening is a proactive management process that requires the examination of the honesty, integrity and trustworthiness (HIT factor) of all individuals working at the CBSA[1] to protect the Agency's personnel, assets and information. It involves the use of various checks and assessments which are conducted as part of the Reliability Status screening process, which is the foundation for all personnel security screenings. The level of security screening required is dependent upon the security level of information and assets that will be accessed in the normal performance of assigned job duties or during the contracting process.

This process involves:

- Determining the type and level of screening required;
- Identifying the types of verifications required;
- Obtaining consent;
- Processing verifications and assessments;

[1] This includes all applicants to and employees (permanent, term, casual, part-time) of the CBSA, contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students.







- Evaluating results of verifications and assessments;
- Granting or denying a reliability status or security clearance ;
- Making the appointment, awarding the contract or entering into a written collaborative agreement; and
- Providing a briefing to the screened individual.

**Definitions**

Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

**Authorities**

This Standard is issued under section 7 (1) and section 12 (1)(e) of the *Financial Administration Act*. It is to be read in conjunction with:

- The appendices to this Standard
- The CBSA Security Volume, and specifically the Policy on Professional Standards Investigations

**Objective**

The objective of this standard is to ensure that the Agency can effectively meet the requirements set forth in its Personnel Security Screening Section (PSSS) to ensure that individuals are cleared to the appropriate level should they meet the screening criteria, which are:

- Determining the honesty, integrity, trustworthiness and reliability of individuals who will have access to government assets, information, networks and government facilities;
- Preventing malicious activity and unauthorized disclosure of Protected and Classified information by an individual in a position of trust;
- Ensuring the loyalty to Canada of individuals who will have access to Classified information and highly critical assets;
- Protecting itself from foreign intelligence gathering and terrorism, or from those who are engaged in other activities viewed as being threats to the security of Canada, as defined in Part II, 21 (2) of the *Canadian Security Intelligence Service (CSIS) Act*; and
- Denying access to government assets and information to individuals involved in criminal acts which are considered to pose an unacceptable risk to the Agency

**Process**

In addition to the baseline verifications of employment history, credit and criminal record checks, all individuals applying to the CBSA, as well as all employees of the CSBA undergoing a renewal or upgrade of their screening, will also undergo the following verifications:

- Law Enforcement Record Checks;







- Internal data base checks;
- Integrity Interviews for new uniformed officers and case by case for others; and
- Other checks may be undertaken for cause on a case by case basis.

There are two types of Personnel Security Screenings: an assessment of reliability; and an assessment of loyalty and reliability related to loyalty. The types and levels of Personnel Security Screening which apply to the CBSA and are as follows:

***CBSA Reliability Status*** indicates the successful completion of reliability checks; allows regular access to government assets with a need to know to protected information.

- Forms required for CBSA Reliability Status:
  - Personnel Screening, Consent and Authorization Form (BSF697E)
  - CBSA Consent Statement (BSF684)

Note: How to complete the Security Clearance Form TBS 330-23

***A Security Clearance***, otherwise known as a Secret or Top Secret is a clearance granted to an individual who requires on a "need to know" basis, access to CLASSIFIED information, assets and/or restricted work sites.

- Forms required for a Security Clearance (in addition to the forms required for a CBSA Reliability Status):
  - Security Clearance Form (TBS/SCT 330-60E)

Note: How to complete the Security Clearance Form TBS 330-60

**Residency & Travel Outside of Canada Questionnaire:** The questionnaire (BSF 641E) is to be completed if an applicant or employee has been out of the country for 180 consecutive days or more within the last 5 years for Reliability Status and 10 years for Security Clearance:

***Note:*** *All armed officers who do not hold a valid Possession and Acquisition Licence (PAL) or who have not yet been screened through the CBSA personnel security screening process, will be screened through this process in advance of their normal renewal cycle.*

New security screening forms are required for the processing of a new screening, renewal of an existing screening, an upgrade or any update to an existing security screening. This includes individuals who have a security screening from another government department.

> *Note:* Any type of extended leave over 18 months requires new forms to be submitted for the processing of an update to an individual's existing security screening. The individual will be







required to complete and submit the forms immediately upon return to work, and may remain in the workplace at the same screening or clearance level that they had when the extended leave commenced, pending the completion of their screening. In cases where there is cause, the individual **may not be** permitted access to CBSA premises, assets, or information until the new screening forms have been processed and a screening is granted. New security screening forms may also be requested from any individual at any time for cause.

**All completed forms required for the individual's specified level of screening need to be submitted to the nearest Regional Security Office for vetting and submission to the CBSA Personnel Security Screening Section for processing.**

**Assessment of Background Checks**

Should adverse information become available through the various checks conducted through the CBSA PSSS, the adverse information shall be considered as per the PGS, with respect to:

- Its nature;
- Seriousness;
- Surrounding circumstances;
- Frequency;
- The willingness of participation;
- The individual's age at the time of the incident(s); and
- The degree of rehabilitation.

Other areas for assessment:

- The honesty, integrity and trustworthiness of the individual (HIT factor)
- Recognition of the seriousness of the misconduct by the employee;
- The aggravating and mitigating factors;
- The possibility this situation was error of judgement (intent/mens rea);
- Other relevant personal circumstances;
- The consequences in terms of injury/potential injury to the organization;
- How would a reasonable person placed in the same context interpret the facts;
- Is the organization ready to accept the level of risk this employee represents;
- Consider the balance of probabilities; and
- Seriousness of the misconduct.

Assessment of Drug Related Offences:

- An applicant may be rejected for:
    - The non-medical use of any illegal drug within the last three years;
    - A history of drug consumption within the last three years;
    - The non-medical use of any drug within the last three years , that was more than occasional or experimental use;
    - The non-medical use of any anabolic steroids, hormones or amphetamines for the purpose of enhancing athletic ability, within the last three years; and
    - Being associated with a person who illegally uses or sells drugs or illegal substances within the last three years or after application.







The severity of drug use can be defined as:

**Experimental use** means that a person consumed a drug six times or less and subsequently terminated the use of any illegal drug.

**Occasional use** means that a person accepts/takes a drug when offered, but does not go out of his/her way to procure it, nor attempt to ensure a regular supply. The occasional user consumes a drug less than once a month.

**Regular use** means frequently using an illegal drug once a month or more.

**Abuse** means the intentional use of any illegal drug or misuse of a prescription or non-prescription drug which within the last three years that has led to significant impairment or distress, including use in a hazardous fashion, continued use despite problems, or failure to fulfill major role obligations at work, school or in the family.

**Dependent use** means a pattern or regular use of an illegal, prescription or non-prescription drug which indicates a physical or emotional need to experience its effects or to avoid the discomfort of its absence. It is associated with an inability to reduce the use of drugs, continued use despite negative consequences (e.g. legal, financial or family). A great deal of time is spent getting or using the drug and important social, occupational, or recreational activities are given up or reduced because of drug use.

All drug related offences will be reviewed on a case by case basis using the above criteria in the decision making process.

The presence of adverse information on a file does not necessarily mean that an individual's screening will be denied or revoked. Each file is reviewed based on its own merits and criteria and a global assessment is conducted, where all information gathered for personnel security screening purposes is evaluated.

**Consequences**

CBSA employees are held to high standards based on the nature of the work they do. There is a requirement for CBSA employees to have honesty, integrity and trustworthiness – the HIT factor. CBSA employees who are found to have breached the HIT factor, CBSA Code of Conduct, the Policy on Government Security or the Values and Ethics Code or any other applicable CBSA policies or standards, will be subject to disciplinary measures based on the seriousness of the misconduct and in accordance with the CBSA Discipline Policy. In some cases this may mean a review and possibly a revocation of the CBSA Reliability Status.

An individual who has been denied or revoked a Reliability Status may not re-apply until after a two year period has passed and the HIT factor has been met. This does not mean that the individual who is re-applying will necessarily be granted a screening but rather allows an opportunity for them to re-submit an application to the CBSA. All re-applications will be reviewed on their own merits and criteria.







**Personnel Security Screening Service Standards**

Reliability Status: 20 business days

Secret Clearance: 60 business days

Top Secret Clearance: 75 business days

**References**

- Policy on Government Security
- Standard on Security Screening

**Enquiries**

For further information, please contact:
Security and Professional Standards Directorate
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Or

For questions regarding the Personnel Security Screening Process, please contact your Regional / Headquarters Security Manager.





# Norme d'enquêtes de sécurité sur le personnel de l'ASFC





**But**

Le but de cette norme est de veiller à ce que, conformément à la Politique sur la sécurité du gouvernement (PSG), l'Agence des services frontaliers du Canada (ASFC) s'assure que toutes les personnes ayant accès aux renseignements et aux biens du gouvernement font l'objet d'enquêtes de sécurité au niveau approprié avant le début de leurs fonctions. L'ASFC procède à ses enquêtes de sécurité sur le personnel conformément à la Norme sur la sécurité du personnel de la PSG et, en outre, l'ASFC procède à des vérifications des antécédents qui lui sont spécifiques, approuvées par le Conseil du Trésor, concernant la cote de fiabilité.

**Date d'entrée en vigueur**

Cette politique entre en vigueur le 6 janvier 2015.

**Application**

Cette norme d'enquêtes s'applique à :

- toutes les personnes qui auront accès aux renseignements et aux biens de l'Agence des services frontaliers du Canada (ASFC);
- tous les postulants à l'ASFC et aux employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), au personnel contractuel et au personnel d'agences privées, ainsi qu'aux personnes en détachement ou en affectation à l'ASFC, y compris les étudiants.

**Contexte**

L'enquête de sécurité sur le personnel est un processus de gestion proactif qui nécessite l'examen de l'honnêteté, de l'intégrité et de la fiabilité (« facteur HIF ») de toutes les personnes travaillant à l'ASFC [1] afin de protéger le personnel, les biens et les renseignements de l'Agence. Elle donne lieu à l'utilisation de divers contrôles et d'évaluations menés dans le cadre du processus d'enquête de sécurité en vue de l'obtention d'une cote de fiabilité, ce qui est le fondement de toutes les enquêtes de sécurité sur le personnel. Le niveau d'enquête de sécurité dépend du niveau de sécurité accordé aux renseignements et aux biens auxquels les personnes visées auront accès dans l'exécution régulière de leurs fonctions ou de leurs obligations contractuelles.

[1] Cela s'applique à tous les postulants à l'ASFC et aux employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), au personnel contractuel et au personnel d'agences privées, ainsi qu'aux personnes en détachement ou en affectation à l'ASFC (y compris les étudiants).





Ce processus comprend :

- la détermination du type et du niveau d'enquête requis;
- le relevé des types de vérification requis;
- l'obtention du consentement;
- le traitement des vérifications et des évaluations;
- l'analyse des résultats des vérifications et des évaluations de sécurité;
- l'attribution ou le refus de la cote de fiabilité ou de la cote de sécurité;
- la nomination, l'attribution du marché ou la conclusion d'un accord écrit de collaboration;
- l'initiation des personnes ayant fait l'objet d'une enquête.

**Définitions**

Des définitions précises provenant de sources qui font autorité se trouvent à au Lexique de la terminologie en sécurité.

**Autorités**

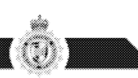
La présente norme est publiée en vertu du paragraphe 7(1) et de l'alinéa 12(1)*e)* de la *Loi sur la gestion des finances publiques*. Elle doit être lue conjointement avec :

- les annexes à la présente norme,
- le Volume de sécurité de l'ASFC, et spécifiquement la politique enquêtes visant les normes professionnelles

**Objectif**

L'objectif de cette norme est de s'assurer que l'Agence peut répondre efficacement aux exigences énoncées dans son programme d'enquête de sécurité sur le personnel, de veiller à ce que les personnes aient le niveau d'autorisation de sécurité approprié, si elles répondent aux critères de vérification de sécurité, qui sont les suivants :

- déterminer la fiabilité, l'honnêteté, l'intégrité, et la loyauté des personnes qui auront accès aux biens de l'État, aux renseignements, aux réseaux et installations gouvernementales;
- prévenir les activités malveillantes et la divulgation non autorisée de renseignements protégés et classifiés par une personne en position de confiance;
- assurer la loyauté envers le Canada de personnes qui auront accès à des renseignements classifiés et à des biens particulièrement essentiels;
- se protéger contre les services de renseignements étrangers et contre le terrorisme, ou contre ceux qui sont engagés dans d'autres activités considérées comme étant des menaces envers la sécurité du Canada, telles qu'elles sont définies à la Partie II, 21(2) de la *Loi sur le Service canadien du renseignement de sécurité (SCRS)* ; et





- refuser l'accès aux biens et aux renseignements du gouvernement aux personnes participant à des actes criminels, présentant un risque inacceptable pour l'Agence.

**Processus**

En plus des vérifications de base des antécédents professionnels, du crédit et du casier judiciaire, toutes les personnes qui postulent à un poste au sein de l'ASFC ainsi que tous les employés de l'ASFC dont la cote de sécurité fait l'objet du renouvellement ou du reclassement subiront également les vérifications suivantes :

- les vérifications des bases de données de l'exécution de la loi;
- les vérifications des bases de données internes;
- entrevues d'intégrité pour les nouveaux agents en uniforme et au cas par cas pour les autres ; et
- d'autres vérifications pouvant être effectuées pour un motif valable, au cas par cas.

Il existe deux types d'enquêtes de sécurité sur le personnel : l'évaluation de la fiabilité et l'évaluation de la loyauté et de la fiabilité relative à la loyauté. Les types et les niveaux d'enquêtes de sécurité sur le personnel qui s'appliquent à l'ASFC sont les suivants :

***La cote de fiabilité de l'ASFC*** indique la réussite des vérifications de la fiabilité de la personne, lui permet l'accès régulier aux biens de l'État et, lorsqu'elle a « besoin de connaître », aux renseignements protégés.

- Formulaires requis pour la cote de fiabilité de l'ASFC :
    - formulaire de vérification de sécurité, de consentement et d'autorisation de personnel (BSF697F)
    - déclaration de consentement de l'ASFC (BSF684)

Notez : Comment remplir le formulaire de vérification de sécurité BSF697F

***Une cote de sécurité,*** aussi connue sous les termes « Secret » et « Très secret », est une cote accordée à une personne ayant « besoin de connaître » pour accéder à des renseignements et des biens CLASSIFIÉS et des établissements de travail dont l'accès est réglementé.

- Formulaires requis pour la cote de sécurité (en plus des formulaires requis pour la cote de fiabilité de l'ASFC) :
    - Formulaire d'autorisation de sécurité (SCT / TBS 330-60F)

Notez : Comment remplir le formulaire d'autorisation de sécurité SCT 330-60





**Questionnaire pour les personnes ayant résidé ou voyagé à l'extérieur du Canada :** Ce questionnaire (BSF641F) doit être rempli si un candidat ou un employé a été à l'extérieur du pays pendant 180 jours consécutifs ou plus au cours des cinq dernières années pour une cote de fiabilité ou dix dernières années pour une cote de sécurité :

***Notez :** Tous les agents armés dont le permis de possession et d'acquisition (PPA) a expiré ou qui n'ont pas encore été évalués selon le processus d'enquête de sécurité sur le personnel de l'ASFC, seront soumis à ce processus à l'avance du cycle normal de renouvellement de leur permis.*

De nouveaux formulaires d'enquête de sécurité sont nécessaires pour le traitement d'une nouvelle enquête de sécurité sur le personnel, le renouvellement, le relèvement ou la mise à jour d'une cote de sécurité actuelle. Ceci comprend les personnes ayant obtenu une cote de sécurité d'un autre ministère.

*Notez : Pour tout type de congé prolongé de plus de 18 mois, de nouveaux formulaires doivent être soumis pour le traitement de la mise à jour de la cote de sécurité actuelle de la personne. La personne devra remplir et soumettre les formulaires dès son retour au travail, et peut demeurer dans le lieu de travail au même niveau de sécurité qu'elle avait au début de son congé prolongé, en attendant son enquête de sécurité. Pour des motifs valables, la personne pourrait ne pas avoir accès aux locaux, aux biens ou aux renseignements de l'ASFC avant que les formulaires d'enquête de sécurité soient traités et que la cote de sécurité soit accordée. Les nouveaux formulaires d'enquête de sécurité peuvent être demandés par toute personne, à tout moment, pour des motifs valables.*

**Tous les formulaires dûment remplis, requis pour le niveau d'enquête de sécurité établi pour le requérant, doivent être déposés au bureau régional de la sécurité le plus proche pour vérification et soumission à la Section des enquêtes de sécurité sur le personnel de l'ASFC aux fins de traitement.**

**Évaluation des vérifications des antécédents**

Si des renseignements défavorables sont découverts au cours des différentes vérifications effectuées dans le cadre de l'enquête de sécurité sur le personnel de l'ASFC, ces renseignements doivent être évalués conformément à la Politique sur la sécurité du gouvernement, en ce qui concerne :
- leur nature;
- leur gravité;
- les circonstances;
- la fréquence;
- la préméditation;
- l'âge de la personne au moment de l'incident;
- son degré de réhabilitation.

Autres domaines évalués :

- l'honnêteté, l'intégrité et la fiabilité de la personne;
- la reconnaissance de la gravité de la faute commise par l'employé;
- les facteurs aggravants et atténuants;
- la possibilité que cette situation ait été une erreur de jugement (intention/*mens rea*);
- d'autres éléments pertinents de la situation personnelle de l'employé;
- les conséquences en ce qui concerne le préjudice/risque de préjudice pour l'organisation;
- la façon dont une personne raisonnable se trouvant dans une situation semblable interpréterait les faits;
- l'organisation est-elle prête à accepter le niveau de risque que cet employé représente;
- la prise en compte de la prépondérance des probabilités;
- la gravité de l'inconduite.

Évaluation des infractions en matière de drogue :

- Une demande peut être refusée pour les raisons suivantes :
  - l'usage non médical de toute drogue illicite au cours des trois dernières années ;
  - des antécédents de consommation de drogues au cours des trois dernières années ;
  - l'usage non médical de toute drogue, au cours des trois dernières années qui était un usage plus qu'occasionnel ou expérimental ;
  - l'usage non médical de tout stéroïde anabolisant, hormone ou amphétamine dans le but d'améliorer la performance athlétique, au cours des trois dernières années ;
  - s'être associé à une personne qui consomme ou vend des drogues ou des substances illicites au cours des trois dernières années ou après avoir fait la demande.

La gravité de l'usage de drogue se définit comme suit :

**Usage expérimental** signifie qu'une personne a consommé de la drogue moins de six fois et à par la suite cessé de consommer toute drogue illicite.

**Usage occasionnel** signifie qu'une personne accepte ou prend de la drogue qui lui est offerte, mais n'entreprend pas de démarches pour s'en procurer et/ou ne tente pas d'assurer un approvisionnement régulier. Le consommateur occasionnel consomme une drogue moins d'une fois par mois.

**Usage régulier** signifie la consommation de drogue illicite une ou plusieurs fois par mois.

**Abus** signifie l'utilisation intentionnelle de toute drogue illicite ou le mauvais usage de drogues prescrites ou non prescrites au cours des trois dernières années ayant donné lieu à une déficience ou une détresse importante, y compris l'usage d'une manière dangereuse, l'usage continu malgré les problèmes ou le défaut de respecter les principales responsabilités au travail, à l'école ou dans la famille.

**Usage créant une dépendance** signifie une tendance ou l'usage régulier de drogues illicites, prescrites ou non prescrites indiquant un besoin physique ou émotionnel de ressentir ses effets ou d'éviter le désagrément de son absence. Il est lié à l'incapacité de réduire l'usage de drogues, l'usage continue de drogues malgré les conséquences négatives (légales, financières ou familiales). Beaucoup de temps consacré à obtenir ou à consommer la drogue et les activités sociales, professionnelles ou récréatives importantes sont abandonnées ou réduites en raison de l'usage de drogues.

Toutes infractions liées à la drogue seront examinées cas par cas à l'aide des critères susmentionnés dans le processus de décision.

La présence de renseignements défavorables dans un dossier ne signifie pas nécessairement que l'enquête de sécurité sur une personne se soldera par un refus ou une révocation. Chaque dossier est examiné en fonction de ses propres mérites et critères et une évaluation globale est effectuée. Tout renseignement recueilli aux fins de l'enquête de sécurité sur le personnel est évalué.

**Conséquences**

Les employés de l'ASFC sont tenus de respecter des normes élevées en raison de la nature du travail qu'ils font. Ils doivent faire preuve d'honnêteté, d'intégrité et de fiabilité - le « facteur HIF ». Les employés de l'ASFC ayant violé les principes du « facteur HIF », le Code de conduite de l'ASFC , la Politique sur la sécurité du gouvernement ou le Code de valeurs et d'éthique, ou d'autres politiques ou normes applicables de l'ASFC, feront l'objet de mesures disciplinaires selon la gravité de l'inconduite, conformément à la Politique en matière de discipline de l'ASFC. Dans certains cas, il peut s'agir d'une révision et peut-être d'une révocation de la cote de fiabilité de l'ASFC.

Un individu don sa cote de fiabilité a été refusé ou révoqué ne peut soumettre une nouvelle demande qu'après une période de deux ans et que l'honnêteté, l'intégrité et la fiabilité de la personne a été atteint. Ceci ne veut pas nécessairement dire que la personne va avoir sa cote de fiabilité rétablie, mais lui donne la chance de soumettre une nouvelle demande à l'ASFC. Toutes les nouvelles demandes seront évaluées par rapport à leurs propres mérites et critères.

**Normes de service des enquêtes de sécurité sur le personnel**

Cote de fiabilité : 20 jours ouvrables

Cote de sécurité de niveau secret : 60 jours ouvrables

Cote de sécurité de niveau très secret : 75 jours ouvrables

**Références**





- Politique sur la sécurité du gouvernement
- Norme sur le filtrage de sécurité

**Demandes de renseignements**

Pour plus d'informations, veuillez-vous adresser à :
Direction de la sécurité et des normes professionnelles
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Ou

Pour des questions concernant le processus d'enquête de sécurité sur le personnel, veuillez communiquer avec votre gestionnaire de la sécurité de la région/de l'Administration centrale




PROTECTED A when completed
PROTÉGÉ A une fois rempli

# SECURITY BRIEFING
## CBSA Employees

As mandated by the Policy on Government Security, I, the undersigned, am responsible for ensuring that you are provided with a security briefing upon commencement of your duties with the CBSA.

All employees of the CBSA must accept security as an important and individual responsibility and therefore, must adequately safeguard sensitive (Classified/Protected) information and valuable assets.

You are required to take the Mandatory Online Security Awareness Modules for all Employees and Managers within 10 business days of commencement of duties, and abide by all security requirements.

All CBSA online training must be accessed and completed through the Self Service Portal via My Learning which will automatically update the employee's training history.

You are also required to review the CBSA Code of Conduct and the Values and Ethics Code for the Public Sector within 10 business days of commencement of duties, and abide by both codes.

**CBSA Assets**

- You must not use property, equipment, materials, vehicles or facilities purchased, used or leased by the CBSA for other than official purposes, unless you have received proper management authorization.
- You are expected to account for and protect any government property and valuables that you possess or control. If any item is lost, stolen or damaged, you must immediately report the incident to your manager or security official.
- You must use badges, official identification and officer or office stamps only for the purposes for which they were intended and in the best interests of the CBSA.
- You are prohibited from using your job title, badge or any other official identification to obtain or appear to obtain any privilege, favor for yourself or others, or to do anything that is illegal, improper or against the best interests of the CBSA.
- If your badge, stamp or official identification is lost, stolen or damaged, you must immediately report the occurrence to your manager or security official.
- If you are temporarily or permanently reassigned and your new functions do not require the use of a badge, stamp or official identification, you must return them to Security. Applicable policies dictate when these assets must be returned.



Initials:_______

## Understanding Classification of Information

**Security classification flows with the information**

- The originator of a document decides on the level of security classification of the document. To assist you with classifying a document, please refer to the links below.
- The receiver of the document must accept the assigned security classification. It cannot be modified without the consent of the Originator. · Information received by CBSA from the public must be assessed and assigned either as Unclassified, Protected A, B or C or Confidential, Secret, Top Secret.
- When creating a new document using information from classified or protected documents or other media, ensure that the new document is also classified at level of the highest source. For example, the document may be deemed Protected B but there is mention of one subject matter at the Secret Level. This would render the document to be classified at Secret.
- Never over-classify a document (e.g., to bring attention to your documents) - it is inappropriate, costly and it can prohibit access to those who need to know.
- Report breaches of information protection immediately to your manager or security official.

Retain a copy of the followings documents: Procedures for Identification, Categorization and Marking of Information Assets

**Do not use** Classified or Protected categories to:

- conceal violations of law, inefficiency, administrative error; or
- to avoid embarrassment or restrain competition.

**Collection, Use, Sharing, Storage, Disclosure, Distribution and Disposal of CBSA Information**

- When you took the Oath of Office and Secrecy/Solemn Affirmation of Office and Secrecy, you swore or affirmed that you would not disclose or make known any matter that comes to your knowledge by reason of your employment.
- You must keep in strict confidence all information you obtain about the CBSA's clients and all other official information to which the public does not have access. This includes information about policies, programs, practices and procedures to which the public does not have official access.
- You cannot access information (files, database, etc.) for personal use.
- You cannot run queries on yourself under any circumstances or queries on others for unauthorized purposes.
- You may disclose CBSA information to clients or designated representatives only if specifically authorized by legislative or departmental guidelines. For example, you can only disclose customs information by applying Section 107 of the Customs Act - Disclosure of Information. Another example would be the disclosure of immigration information under the Immigration and Refugee Protection Act and the Privacy Act.
- Refer to the Sections 7 through 10 of the Immigration and Refugee Protection Act - Agreements, which provide the authority to disclose information to certain individuals for the purposes of enforcing the Act.

 Initials:_______

**Need to Know Principle**

You should have a complete understanding of the “Need to Know” principle.

- You may access official information only if authorized and required for the purposes of enforcing applicable legislation and only when you have the appropriate security screening level to access it. For example, in order to access Protected B information, you must have a valid Reliability Status. In order to access Secret information, you must have a valid Secret Clearance.
- Under no circumstances may you access official information for personal use, gain or financial benefit for yourself, your relatives or anyone else.
- You are authorized to share official information only to those who have a need to know to support their functions. You must also ensure they have the appropriate security screening level to receive the information.
  - You are required to safeguard official information and must use, process, store and handle designated or classified information only for purposes specified by the CBSA. You may not remove, hide, change, mutilate, copy or destroy any official information.
  - You are prohibited from destroying, altering, falsifying or concealing a record, or directing anyone to do so, with the intent of obstructing the right of access set out in section 67.1 of the Access to Information Act or disclosing any personal information without proper authorization as set out in the Privacy Act.

Keep in Mind:

- The information doesn't become less sensitive because you no longer require the document.
- If you are known to have sensitive information, your waste basket is the first place someone may look for information of interest.
- Never place boxes of documents for shredding in public areas. (For example, near an elevator or an entrance).

Also keep in mind:

- Discussions can easily be overheard.
- If you talk at a normal level, can you be heard through the walls or in the hallway?
- If you are talking in your office, are there people (cleaners / contractors) around who can hear you?

Great care should be exercised when discussing or accessing sensitive information especially:

- In public places, including cafeterias and public transit; · outside your own office area (cubicles);
- At meetings, when you are unsure who is in attendance; and
- Reading documents while in transit (bus, plane).
- When you leave the employment of the CBSA, you cannot take with you or retain any CBSA records or documents, including paper documents, CDs, USB sticks and diskettes with electronic information, video, etc., unless authorized by your manager.

 Initials:_______

- You must cooperate and assist in the conduct of governmental investigations such as an investigation conducted by the Personnel Security and Professional Standards Division, the Public Sector Integrity Commissioner, or a Health and Safety Officer who is carrying out his or her duty under the Canada Labour Code. You must provide information and complete access to the CBSA information systems, documents and records to an investigator to the extent that such access is legally permitted.
- You are required to give testimony on behalf of the CBSA or the Crown in court and/or before any administrative tribunal or panel. While you are obligated to assist in ongoing investigations under Government of Canada legislation, you should consult your manager before assisting a provincial or foreign authority.

***Security of Information Act, Part II of Bill C-36 Entitled the Anti-terrorism Act***
18. (1) Every person with a security clearance given by the Government of Canada commits an offence who, intentionally and without lawful authority, communicates or agrees to communicate, to a foreign entity or to a terrorist group any information that is of a type that the Government of Canada is taking measures to safeguard.
(2) Every person who commits an offence under subsection (1) is guilty of an offence and is liable to imprisonment for a term of not more than 2 years.

## Electronic Network Access and Uses

If you have access to, or use the CBSA's computer systems, equipment or software, you must make every effort to protect the CBSA from any possible threats to security by, in particular:

- guarding against accidental or deliberate destruction of data and equipment; unauthorized disclosure of sensitive information; theft and corruption; and exposure to viruses;
- assigning access identification and passwords to your system;
- following CBSA policies and procedures regarding the access restrictions to data banks and the posting of information;
- following CBSA policies and procedures regarding the purchase and use of software and other systems use, including complying with security restrictions; and
- not storing classified or protected information on removable hard drives, USB sticks or any other media devices (CD, DVD, etc.);
- immediately reporting any breach of computer security, policies or standards to your manager.

**Note:** CBSA computer systems or those of external agencies accessed via the CBSA's network, software, equipment, networks, Internet, intranet and e-mail are for authorized business purposes only.

However, limited personal use of the Internet, intranet and e-mail is permitted provided it complies with all related legislation, policies and guidelines, does not affect your productivity or that of your colleagues, and imposes no storage burden on the CBSA computer systems. Examples of acceptable limited personal use include professional activities, career development, or reading or writing a brief e-mail after hours or during a lunch break.

**Travelling Abroad with electronic devices**
**You should be aware:**

Many countries monitor communication via public places, in hotels, restaurants/bars/cafes, government offices and even airports. Privacy laws do not exist in many countries. Information transmitted via wireless devices is vulnerable to being intercepted. Any information shared by means of fax transmittals, personal digital assistants, computers, telephone or any electronic devices can be intercepted. Be aware of this when you are transmitting government and/or personal information from abroad

 Initials:_______

**Before Travelling:**
If your electronic devices are not required to conduct official government business, then do not take them with you in your travels. Do not bring additional work related information with you if it is not needed. Keep in mind the consequences if your information were to be stolen or compromised by a foreign government. If you must carry your devices, prepare them by creating a strong password with special characters/numbers, change your password periodically and upon return home, and install through Information Technology Officials up-to-date antivirus and firewall protection.

**While travelling:**
Do not store your devices in your checked baggage. Always transport your devices in your carry-on luggage. Enable digital signature and encryption capabilities if possible.
Your electronic devices should never be left unattended. Should you need to store them, the battery and sim card should be removed and stored in a different safe location.

**Reporting Security Incidents**
You must immediately notify your manager or a security officer if you become aware of:

- a security infraction;
- a negligent or criminal act;
- an unsafe or hazardous condition at work;
- an accident or injury to yourself or other employees;
- a failure on the part of any employee to observe workplace safety and security standards, rules and procedures; and/or
- a breach of CBSA information.

## CBSA Code of Conduct

**Private, Off-Duty Conduct and Outside Activities**
Your outside activities and off-duty conduct are usually private matters. They could become work-related matters, however, if they have negative consequences on the Agency. **You must avoid such activities, which may include those that:**

- reflect negatively on the Agency, its employees (including its managers) or its programs;
- render you unable to perform a requirement of your duties;
- lead other employees to refuse, be reluctant or be unable to work with you;
- render you guilty of a breach of the Criminal Code; and
- make it difficult for the Agency to manage its operations efficiently and/or to direct its workforce.

You must also avoid activities that place you or the Agency at risk by knowingly associating, outside of your official duties, with individuals or groups who are believed or suspected to be connected with criminal activities.

**Caution:** You are not permitted to do anything illegal or contrary to the Criminal Code, the CBSA Act, or any legislation or regulation enforced by the Agency. **In the unlikely event of being arrested, detained or charged** - in Canada or outside Canada - with a violation of laws or regulations, **you must immediately report this incident to your manager**. This includes minor incidents, such as a traffic violation or Highway Code violation ticket received while using a government-owned or leased vehicle. You must also **report to your manager, any contact or associations you have with known or suspected criminals outside your official duties**, so that you can protect yourself and the Agency.

**Misconduct**

You must promptly report to your immediate Supervisor or Manager, or to their Director (if the circumstances warrant) any allegation or suspicion of misconduct, criminal or otherwise, by an employee **(including yourself)** that you are aware of, or have witnessed.

**Attach additional briefing material to support specific security requirements related to functions within the Employee's Section.**

**In support of your security screening**

- All employees of the CBSA must ensure they hold a valid security screening at the appropriate level. It is your responsibility to advise your immediate Supervisor or Security Official of any changes to your circumstances which could affect your current security screening. For example:
  - You have been previously granted a Secret or Top Secret Clearance and you subsequently get married, or remarried, or you commence a common-law relationship. In these cases, a new Security Clearance Form TBS-330-60 must be completed and submitted to Security.
  - There is a requirement for you to access information at a higher level than the security screening level granted to you. For example, you are cleared to Reliability and your functions will require you to access Secret information.
  - If anyone in your personal life shows unusual interest in your work or they approach you and ask you to disclose information or help them facilitate the entry of goods or persons.
  - Any incidents which may compromise your position such as attempts at coercion by the criminal element.
  - Any incidents where unauthorized individuals are seeking access to sensitive information or where there is concern that you may be the target of an attempted exploitation.
  - If you have any new criminal charges, convictions, and/or police involvement.

**Take these simple steps to ensure you are applying the proper security safeguards**

- Ensure you keep attractive and sensitive items (including personal items) out of sight. Consider a clean desk best practice.
- Make sure you lock up sensitive information and do not leave it in the open. Our Physical Security organization can assist you with this.
- Ensure that appropriate technology is being used to process sensitive material. Our COMSEC organization can assist you with this.

 Initials:_______

- Know the sensitivity of information you are handling. If you receive something and are unsure of the sensitivity of the information, contact the originator and ask. Classify documents appropriately.
- Ensure that you have a routine for the disposal of sensitive information. Use an appropriate shredder to destroy protected and classified documents.
- Ensure you have a password on your screensaver and log off at night.
- Ensure you wear your ID card and/or Badge Identifier visibly.
- Ensure you do not store classified or protected information on removable hard drives, USB sticks or any media devices (CD, DVD, etc.).
- Ensure you are not taking sensitive or classified CBSA information home with you at the end of the work day unless you have an approved container for transport and storage of the information. This includes information in paper and electronic format.
- Ensure you report security issues (Form BSF152) to your manager and seek advice from Security.
- Visitors must be escorted at all times.
- Any unfamiliar person encountered within your work space should be politely challenged.
- Place an “Away from the office” security notice in plain view warning individuals not to leave sensitive documents in your workstation.
- Never share your network password.
- Do not install software or hardware without IT authorization.
- You must report to a CBSA supervisor or manager any new criminal conviction(s) and/or police involvement including when charges have been laid that are directly related to you.

 Initials:_______

| Acknowledgement and Employee Signature Authentication | |
|---|---|
| I fully understand and agree to comply with the above statutory and administrative requirements. I fully understand and agree that failure on my part to comply may result in my being subject to a review and possibly a revocation of the CBSA Reliability Status, disciplinary action, up to and including termination of employment.<br><br>I, the undersigned attest that the signatures placed on the security screening forms TBS/SCT 330-23 and TBS/SCT 330-60 completed by me and submitted to the Canada Border Services Agency are my own and are true and authentic. | |
| **Name of Employee (print)** | **Region/Branch** |
| **Title** | |
| **Signature** | **Date (yyyy-mm-dd)** |

| CBSA Briefing Official | |
|---|---|
| This briefing was provided to the Individual identified above. A Security Screening Certificate and Briefing Form (ref: TBS330-47) was read and signed by the employee. As the Briefing Official, I have completed Part D of the form TBS/SCT330-47 and I have provided the employee with a copy of the signed briefing document and a copy of form TBS/SCT330-47. | |
| **Name (print)** | **Region/Branch** |
| **Title** | |
| **Signature** | **Date (yyyy-mm-dd)** |

**Note:** This signed CBSA Employee Briefing Form must be returned to the Personnel Security Section in Headquarters along with the signed Security Screening Certificate and Briefing Form TBS/SCT 330-47.

**BSF769E**




PROTÉGÉ A une fois rempli
PROTECTED A when completed

**SÉANCE D'INFORMATION SUR LA SÉCURITÉ**
**Employés de l'AFSC**

En vertu de la Politique du gouvernement sur la sécurité, je, soussigné, suis chargé de veiller à ce que vous participiez à une séance d'information sur la sécurité à votre entrée en fonction à l'Agence des services frontaliers du Canada (ASFC).

Tous les employés de l'ASFC doivent accepter que la sécurité est une responsabilité importante et individuelle, et ils devront donc protéger adéquatement les renseignements de nature délicate (classifiés/protégés) et les biens de valeur.

Vous devez faire les **Modules en ligne obligatoires de sensibilisation à la sécurité** pour tous les employés et les gestionnaires dans les dix jours ouvrables de votre entrée en fonction et respecter toutes les règles de sécurité. Il faut faire toute la formation en ligne de l'ASFC en accédant au Portail libre-service dans Mon apprentissage; ainsi, l'historique de la formation suivie par l'employé sera automatiquement mise à jour.

De plus, vous devez étudier le **Code de conduite - de l'ASFC** et le **Code de valeurs et d'éthique du secteur public** dans les dix jours ouvrables de votre entrée en fonction et les respecter.

**Biens de l'ASFC**

- Vous ne devez pas utiliser des biens, de l'équipement, du matériel, des véhicules ou des installations achetés, utilisés ou loués par l'ASFC à des fins autres qu'officielles, à moins que vous n'ayez reçu l'autorisation appropriée de la direction.
- Vous êtes responsable de la conservation et de la protection des biens et des articles de valeur du gouvernement que vous détenez ou contrôlez. Si un article est perdu, volé ou endommagé, vous devez immédiatement signaler l'incident à votre gestionnaire ou à un responsable de la sécurité.
- Vous devez utiliser les insignes, les pièces d'identité officielles et les estampilles de bureau ou d'agent uniquement aux fins auxquelles ils sont destinés et dans le meilleur intérêt de l'ASFC.
- Il vous est interdit d'utiliser votre titre de poste, votre insigne ou toute autre pièce d'identité officielle pour obtenir ou sembler obtenir un privilège ou une faveur pour vous-même ou pour d'autres personnes, ou pour faire quoi que ce soit d'illégal ou d'inapproprié, ou qui n'est pas dans le meilleur intérêt de l'ASFC.
- Si vous avez perdu ou endommagé votre insigne, votre estampille ou votre pièce d'identité officielle, ou qu'ils ont été volés, vous devez en aviser immédiatement votre gestionnaire ou un responsable de la sécurité.
- Si vous faites l'objet d'une réaffectation temporaire ou permanente et que vos nouvelles fonctions ne vous obligent pas à utiliser un insigne, une estampille ou une pièce d'identité officielle, vous devez les remettre à la Sécurité. Les politiques applicables dictent quand ces biens doivent être rendus.



Initiales : ______

## Compréhension de la classification des renseignements

**Classification de sécurité liée aux renseignements**

- L'auteur d'un document décide de son niveau de classification. Pour savoir comment classer un document, consultez les liens ci-dessous.
- Le destinataire du document doit accepter la classification de sécurité assignée. Elle ne peut être modifiée sans l'autorisation de l'expéditeur.
- L'information envoyée par le public à l'ASFC doit être évaluée, puis se faire attribuer une classification (non classifié, « Protégé A », « Protégé B », « Protégé C » ou « Confidentiel », « Secret », « Très secret »).
- Lorsque vous créez un nouveau document en vous servant de renseignements se trouvant dans des documents ou d'autres médias protégés ou classifiés, assurez-vous que le nouveau document est aussi classifié au niveau de la source pour laquelle la classification est la plus élevée. Par exemple, le document peut être réputé « Protégé B », mais il y est question d'un sujet de niveau secret. Ainsi, l'ensemble du document devrait être classifié « Secret ».
- Il ne faut jamais classifier un document à un niveau trop élevé (p. ex., pour attirer l'attention sur vos documents); cela est inapproprié, dispendieux et peut bloquer l'accès au document à des personnes qui doivent en prendre connaissance.
- Il faut signaler le non-respect de la protection de renseignements immédiatement à votre gestionnaire ou à un responsable de la sécurité. Conservez une copie du document suivant : Procédures d'identification, de catégorisation et de marquage des ressources d'information

**Ne vous servez pas** des catégories « Classifié » ou « Protégé » afin de :

- dissimuler des infractions à la loi, l'inefficacité, une erreur administrative;
- restreindre la compétition ou d'éviter de vous trouver dans l'embarras.

**Collecte, utilisation, échange, entreposage, communication, diffusion et élimination de renseignements de l'ASFC**

- Lorsque vous avez prêté le serment professionnel/affirmation solennelle et engagement au secret professionnel, vous avez juré ou affirmé que vous ne communiqueriez pas/ne rendriez pas publics des éléments dont vous auriez pris connaissance dans le cadre de votre emploi.
- Vous devez conserver de façon strictement confidentielle tous les renseignements que vous obtenez au sujet des clients de l'ASFC, ainsi que tous les autres renseignements officiels auxquels le public n'a pas accès. Cela comprend les renseignements sur les politiques, les programmes, les pratiques et les procédures auxquels le public n'a pas officiellement accès.
- Vous ne pouvez accéder à des renseignements (dossiers, bases de données, etc.) à des fins personnelles.
- Vous ne pouvez en aucun cas mener des enquêtes sur vous-même ou d'autres personnes à des fins non autorisées.
- Vous pouvez communiquer des renseignements classifiés/protégés à des clients ou à des représentants désignés seulement si vous y êtes expressément autorisé par les lignes directrices législatives ou ministérielles. Par exemple, vous ne pouvez communiquer des renseignements douaniers qu'en application **de l'article 107 de la *Loi sur les douanes*** (Communication de renseignements). Un autre exemple serait la communication de renseignements en matière d'immigration en vertu de la *Loi sur l'immigration et la protection des réfugiés* et de la *Loi sur la protection des renseignements personnels*.
- Reportez-vous aux articles 7 à 10 de la ***Loi sur l'immigration et la protection des réfugiés (Concertation intergouvernementale)***, qui permet de communiquer des renseignements à certaines personnes aux fins d'exécution de la Loi.



Initiales : ______

**Principe du besoin de connaître**

Vous devez bien comprendre le principe du besoin de connaître.

- Vous pouvez accéder à des renseignements officiels uniquement si vous y êtes autorisé, si vous avez besoin de ces renseignements pour appliquer les lois pertinentes et si vous avez les autorisations de sécurité appropriées pour ce faire. Par exemple, pour avoir accès à des renseignements « Protégé B », vous devez avoir une cote de fiabilité valide. Pour accéder à des renseignements « Secret », vous devez avoir une cote secrète valide.
- Vous ne pouvez en aucun cas utiliser ces renseignements à des fins personnelles ou pour obtenir un bénéfice ou un avantage financier pour vous-même, un membre de votre famille ou toute autre personne.
- Vous ne pouvez communiquer des renseignements officiels qu'aux personnes ayant besoin de connaître dans le cadre de leurs fonctions. Vous devez aussi vous assurer qu'elles ont la cote de sécurité appropriée pour recevoir les renseignements.
  - Vous êtes tenu de protéger les renseignements officiels et ne devez utiliser, traiter, entreposer et manipuler des renseignements désignés ou classifiés qu'aux fins précisées par l'ASFC. Vous ne pouvez pas effacer, cacher, modifier, tronquer, copier ou détruire des renseignements officiels.
  - Il vous est interdit de détruire, de modifier, de falsifier ou de cacher un document, ou de demander à toute personne de le faire, dans l'intention d'entraver le droit d'accès prévu à l'article 67.1 de la Loi sur l'accès à l'information, ou de communiquer tout renseignement personnel sans l'autorisation prévue par la Loi sur la protection des renseignements personnels.

*Gardez à l'esprit ce qui suit :*

- Les renseignements ne deviennent pas moins délicats parce que vous n'avez plus besoin du document.
- Si l'on sait que vous avez des renseignements délicats, le premier endroit où l'on cherchera des renseignements d'intérêt est votre corbeille à papier.
- Ne placez jamais de boîtes de documents à déchiqueter dans des aires publiques (par exemple, près d'un ascenseur ou d'une entrée).

*De plus, gardez à l'esprit que :*

- Les discussions peuvent être entendues facilement.
- Si vous parlez et que le volume de votre voix est normal, peut-on vous entendre à travers les murs ou dans le corridor?
- Si vous parlez dans votre bureau, y a-t-il des personnes (nettoyeurs/entrepreneurs) aux alentours qui peuvent vous entendre?

Il faut faire très attention lorsque l'on discute de renseignements délicats, en particulier :

- dans un lieu public, notamment dans les cafétérias et les transports en commun;
- à l'extérieur de votre propre aire de bureau (postes de travail modulaires);
- à des réunions, quand vous ne connaissez pas tous les participants;
- dans les moyens de transport en commun (autobus, avion), lorsque vous lisez des document.

- Lorsque vous quittez votre emploi à l'ASFC, vous ne pouvez apporter ou conserver des dossiers ou des documents de l'ASFC, notamment des documents papier, des CD, des clés USB et des disquettes comprenant des renseignements électroniques et des vidéos, à moins que votre gestionnaire ne vous y autorise.

 Initiales : ______

- Vous devez collaborer pour la tenue d'enquêtes gouvernementales comme une enquête effectuée par la Division de la sécurité du personnel et des normes professionnelles, le commissaire à l'intégrité du secteur public ou un agent de santé et sécurité qui s'acquitte de ses fonctions en vertu du Code canadien du travail. Vous devez fournir à l'enquêteur des renseignements et l'accès à tous les dossiers, documents et systèmes d'information de l'ASFC dans la mesure permise par la loi.
- Vous êtes tenu de témoigner pour le compte de l'ASFC ou de la Couronne en cour et/ou devant tout tribunal administratif ou groupe de travail. Bien qu'il vous incombe d'aider à la tenue d'enquêtes en cours en vertu de la législation du gouvernement du Canada, vous devez consulter votre gestionnaire avant de prêter main-forte à une autorité provinciale ou étrangère.

**Loi sur la protection de l'information, partie 2 du projet de loi C-36 intitulé Loi antiterroriste**

18. (1) Commet une infraction le titulaire d'une habilitation de sécurité délivrée par le gouvernement fédéral qui, intentionnellement et sans autorisation légitime, communique des renseignements du type de ceux à l'égard desquels celui-ci prend des mesures de protection à une entité étrangère ou à un groupe terroriste ou accepte de les leur communiquer.

(2) Quiconque commet l'infraction prévue au paragraphe (1) est coupable d'un acte criminel passible d'un emprisonnement maximal de deux ans.

**Accès aux réseaux électroniques et utilisation de ceux-ci**

Si vous avez accès aux systèmes, aux logiciels ou au matériel informatique de l'ASFC ou si vous utilisez ceux-ci, vous ne devez ménager aucun effort pour protéger l'ASFC contre toute menace possible à la sécurité, particulièrement en :

- évitant la destruction accidentelle ou délibérée des données et du matériel, la communication non autorisée de renseignements de nature délicate, le vol et l'altération, ainsi que l'exposition à des virus;
- assignant des codes d'identification et des mots de passe à votre système;
- respectant les politiques et les procédures de l'ASFC en ce qui a trait aux restrictions liées à l'accès aux banques de données, ainsi qu'à l'affichage de renseignements;
- respectant les politiques et les procédures de l'ASFC en ce qui a trait à l'achat et à l'utilisation de logiciels et d'autres systèmes, y compris les restrictions liées à la sécurité;
- n'entreposant pas de renseignements classifiés ou protégés sur des disques durs externes, des clés USB ou autres supports amovibles (CD, DVD, etc.).
- signalant immédiatement à votre gestionnaire toute atteinte à la sécurité, aux politiques ou aux normes informatiques.

**Nota :** Utiliser les systèmes informatiques de l'ASFC et ceux des organismes externes auxquels vous avez accédé par l'entremise des réseaux, des logiciels, du matériel, de l'Internet, de l'intranet et du courrier électronique de l'ASFC seulement pour les fins opérationnelles autorisées.

Cependant, une utilisation limitée à des fins personnelles d'Internet, de l'intranet et du courrier électronique est permise, dans la mesure où elle est conforme à toutes les lois, les politiques et les lignes directrices pertinentes, où elle ne nuit pas à votre productivité ou à celle de vos collègues et où elle n'impose aucun fardeau d'entreposage aux systèmes informatiques de l'ASFC. Au nombre des utilisations à des fins personnelles qui sont acceptables, mentionnons les utilisations aux fins des activités professionnelles, du perfectionnement ou de la lecture ou de la rédaction de brefs courriels après les heures de travail ou pendant une pause.

 Initiales : ______

## Voyager à l'étranger avec des appareils électroniques

**Ce que vous devez savoir**

De nombreux pays surveillent les communications dans les lieux publics, les hôtels, les restaurants/bars/cafés, les bureaux du gouvernement et même les aéroports. Il n'existe pas de loi sur la protection des renseignements personnels dans de nombreux pays. Les renseignements transmis au moyen d'appareils sans fil peuvent être interceptés. Tous les renseignements communiqués par télécopie, assistant numérique personnel, ordinateur, téléphone ou tout autre appareil électronique peuvent être interceptés. Vous devez le savoir lorsque vous transmettez des renseignements personnels ou du gouvernement depuis l'étranger.

**Avant le voyage**

Si vos appareils électroniques ne sont pas nécessaires dans le cadre de vos fonctions officielles, ne les apportez pas avec vous en voyage. N'apportez pas d'autres renseignements liés à votre travail à moins qu'ils ne soient nécessaires. Gardez en tête quelles seraient les conséquences si les renseignements étaient volés ou compromis par un gouvernement étranger. Si vous devez amener vos appareils, préparez-les en établissant un mot de passe fiable contenant des caractères spéciaux/des numéros, changez votre mot de passe régulièrement et, à votre retour, faites installer par des responsables des technologies de l'information un antivirus récent et une protection pare-feu.

**Pendant le voyage**

Ne placez pas vos appareils dans vos bagages enregistrés. Vous devez toujours transporter vos appareils dans votre bagage à main. Vous devez activer votre signature numérique et les fonctions de chiffrement, si possible.

Vos appareils électroniques ne doivent jamais être laissés sans surveillance. Si vous devez les ranger, la pile et la carte SIM devraient être retirées et conservées dans un endroit sécuritaire.

**Signalement des incidents de sécurité**

Vous devez aviser immédiatement votre gestionnaire ou un agent de sécurité si vous constatez ce qui suit :

- une infraction aux règles de la sécurité;
- un acte négligent ou criminel;
- une condition de travail dangereuse ou non sécuritaire;
- un accident ou une blessure à vous-même ou à d'autres employés;
- le manquement d'un employé au respect des normes, des règles et des procédures de sécurité en milieu de travail;
- une fuite de renseignements de l'ASFC.

**Code de conduite de l'ASFC**
**Activités extérieures et conduite en dehors du travail/dans la vie privée**

Vos activités et votre conduite en dehors du travail font habituellement partie de votre vie privée. Cependant, elles peuvent devenir une question reliée au travail s'il y a des conséquences négatives pour l'Agence. Vous devez éviter de telles activités, y compris celles qui :

- nuisent à la réputation de l'Agence, des employés (y compris les gestionnaires) et des programmes;
- vous rendent incapable de remplir une exigence de vos fonctions;
- conduisent d'autres employés à refuser de travailler avec vous, à y être réticents ou à en être incapables;
- vous rendent coupable d'une infraction au Code criminel.
- rendent difficile pour l'Agence la gestion efficace de ses opérations et/ou la direction de son personnel.



Initiales : ______

Vous devez éviter toute activité qui vous rend, ou qui rend l'Agence, vulnérable en vous associant, en dehors de vos fonctions officielles, à des individus ou à des groupes qui sont liés ou sont soupçonnés d'être liés à des activités criminelles.

**AVERTISSEMENT : Il vous est interdit de commettre un acte qui est illégal ou qui contrevient au Code criminel, à la Loi sur l'ASFC ou à toute loi ou règlement appliqué par l'Agence. Si vous êtes arrêté, détenu ou accusé - au Canada ou à l'étranger - d'une infraction à une loi ou à un règlement, vous devez signaler immédiatement l'incident à votre gestionnaire**. Ceci comprend les incidents mineurs, entre autres, une infraction au code de la route au volant d'un véhicule appartenant au gouvernement ou loué par lui. Vous devez aussi **signaler à votre gestionnaire tout contact en dehors du travail avec des individus ou groupes qui sont liés ou sont soupçonnés d'être liés à des activités criminelles** afin de pouvoir vous protéger et protéger l'Agence.

**Inconduite**

Vous devez signaler sans délai à votre superviseur immédiat ou gestionnaire, ou à leur directeur (si la situation le justifie) toute allégation ou tout soupçon d'inconduite, délit criminel ou autre commis par un employé (**incluant vous-même**) dont vous êtes au courant ou avez été témoin.

**Veuillez joindre les documents d'information supplémentaires à l'appui des règles de sécurité particulières liées aux fonctions au sein de la section de l'employé.**

**Pour l'enquête de sécurité**

- Tous les employés de l'ASFC doivent s'assurer d'avoir une cote de sécurité valide au niveau approprié. Vous devez aviser votre superviseur immédiat ou un responsable de la sécurité de tout changement à votre situation qui pourrait avoir des répercussions sur votre niveau de sécurité actuel. Par exemple :
    - Vous avez déjà obtenu une cote « Secret » ou « Très secret », puis vous vous êtes marié ou remarié ou vous avez commencé à vivre en union de fait. Dans ces cas, un nouveau formulaire d'autorisation de sécurité SCT-330-60 doit être rempli et envoyé à la Sécurité.
    - Vous devez accéder à des renseignements qui sont classifiés à un niveau supérieur à celui qui vous a été accordé lors de l'enquête de sécurité. Par exemple, vous avez une cote de fiabilité et, dans le cadre de vos fonctions, vous devez accéder à des renseignements secrets.
    - Quelqu'un dans votre entourage fait preuve d'un intérêt inhabituel envers votre travail ou on vous approche et on vous demande des renseignements ou de l'aide pour faciliter l'entrée de marchandises ou de personnes au Canada.
    - Tout incident qui pourrait compromettre votre poste, comme des tentatives de contrainte par un élément criminel.
    - Tout incident où des personnes non autorisées tentent d'accéder à des renseignements délicats ou toute situation où vous croyez être la cible d'une tentative d'exploitation.
    - Dans le cas de nouvelles accusations au criminel, condamnations et/ou participations policières.



Initiales : ______

**Faites simplement ce qui suit pour appliquer les mesures de sécurité appropriées**

- Assurez-vous de garder les articles attirants et délicats (y compris les articles personnels) hors de la vue. Considérez le rangement de votre bureau comme une pratique exemplaire.
- Veillez à mettre sous clé les renseignements délicats et à ne pas les laisser à la vue. Notre organisme de sécurité matérielle peut aider à ce sujet.
- Assurez-vous que la technologie appropriée est utilisée pour traiter le matériel délicat. Notre organisme de la COMSEC peut vous aider à cet égard.
- Soyez au courant de la classification des renseignements que vous manipulez. Si vous recevez un document et que vous n'êtes pas certain de la classification des renseignements qu'il contient, communiquez avec l'auteur et demandez-lui. Classifiez les documents de manière appropriée.
- Adoptez une routine pour l'élimination des renseignements délicats. Servez-vous d'une déchiqueteuse appropriée pour détruire les documents classifiés et protégés.
- Ayez un mot de passe pour votre économiseur d'écran et fermez votre session le soir.
- Portez votre carte d'identité et/ou votre bande-numéro d'insigne de manière visible.
- Veillez à ne pas entreposer de renseignements classifiés ou protégés sur des disques durs externes, des clés USB ou autres supports amovibles (CD, DVD, etc.).
- Assurez-vous de ne pas apporter à la maison des renseignements de l'ASFC délicats ou classifiés à la fin de la journée de travail à moins d'avoir un contenant approuvé pour le transport et l'entreposage des renseignements. Cela comprend les renseignements sur papier et les renseignements électroniques.
- Signalez les incidents de sécurité (formulaire BSF152) à votre gestionnaire et sollicitez les conseils de la Sécurité.
- Les visiteurs doivent être accompagnés en tout temps.
- Tous les inconnus rencontrés à votre lieu de travail doivent être questionnés poliment.
- Veuillez placer un avis de la sécurité « À l'extérieur du bureau » bien en vue afin d'avertir les gens de ne pas laisser de documents délicats à votre poste de travail.
- Ne communiquez jamais votre mot de passe du réseau.
- N'installez pas de logiciel ou d'équipement sans l'autorisation de la TI.
- Vous devez signaler à un superviseur ou à un gestionnaire de l'ASFC toute condamnation criminelle et/ou participation policière, notamment lorsque des accusations ont été portées et qu'elles sont directement liées à votre personne.



Initiales : ______

| Attestation et Authentification de la signature de l'employé | |
|---|---|
| Je comprends et accepte de respecter les exigences législatives et administratives précitées. Je comprends et je conviens qu'un manquement de ma part à me conformer à ces exigences pourrait entraîner la révision et possiblement la révocation de ma cote de fiabilité, une mesure disciplinaire, et même mener au licenciement.<br><br>Je, soussigné, certifie que les signatures apposées sur les formulaires d'enquête de sécurité TBS/SCT 330-23 et TBS/SCT 330-60 (s'il y a lieu) remplis par moi et envoyés à l'Agence des services frontaliers du Canada sont les miennes et qu'elles sont véritables et authentiques. | |
| **Nom de l'employé (caractères d'imprimerie)** | **Région/Direction générale** |
| **Titre** | |
| **Signature** | **Date (aaaa-mm-jj)** |

| Agent de l'ASFC qui a donné la séance | |
|---|---|
| La séance d'information a été donnée à l'employé ci-dessus. Ce dernier a lu et signé le Certificat d'enquête de sécurité et profil de sécurité (réf. : TBS/SCT 330-47). À titre de responsable de la séance d'information, j'ai rempli la partie D du formulaire TBS/SCT330-47 et j'ai remis à l'employé une copie du document signé et du formulaire TBS/SCT330-47. | |
| **Nom (caractères d'imprimerie)** | **Région/Direction générale** |
| **Titre** | |
| **Signature** | **Date (aaaa-mm-jj)** |

**Nota :** Ce formulaire dûment signé d'information sur la sécurité pour les employés de l'ASFC doit être retourné à la section des enquêtes et des examens de la sécurité de l'Administration centrale, accompagné du Certificat d'enquête de sécurité et profil de sécurité TBS/SCT 330-47 également signé.

**BSF769F**




PROTECTED A when completed
PROTÉGÉ A une fois rempli

# SECURITY BRIEFING
## External Service Providers

As mandated by the Policy on Government Security, I, the undersigned, am responsible for ensuring that you are provided with a security briefing prior to the commencement of your duties with the Canada Border Services Agency (CBSA).

All external service providers working for the CBSA must view security as an important individual responsibility, and therefore, must adequately safeguard sensitive information (Classified/Protected) and valuable assets.

You are required to take the **Online Security Awareness Module** within 10 working days of commencement of duties, and abide by all security requirements.

Please note: The individual being security briefed must provide his/her initials at the bottom of each page and also his\her signature on the last page of this security briefing document upon being briefed or re-briefed by a CBSA official.

**Level Of Security Screening Granted:**

You have been granted the following security screening level:

- ☐ **Secret Clearance**
- ☐ **Reliability Status**
- ☐ **Top Secret Clearance**

**Your Security Responsibilities**

- You are expected to account for and protect all government information/assets, property and valuables that are in your possession or control. If any item is lost, stolen or damaged, you must immediately report the incident to your immediate CBSA supervisor or a CBSA Security Official.
- You must report to a CBSA supervisor any new criminal conviction(s) and/or police involvement including when charges have been laid that are directly related to you.
- If your identification card is lost, stolen or damaged, you must immediately report the occurrence to your immediate CBSA supervisor.
- When you leave the CBSA, you must return your identification card and any other assets belonging to the CBSA.
- You must advise the CBSA if you are no longer employed by the company the CBSA entered into a contract with for your services.



Initials:_______

- Unless authorized by an official of the CBSA, you are prohibited from accessing or reviewing any CBSA information contained in CBSA offices or databases.
- CBSA information (in any format e.g. paper documents, CDs, USB sticks and diskettes video, etc.) cannot leave CBSA premises unless you have received consent from a CBSA supervisor and you have an approved container for transport and storage of the information
- You are prohibited from using CBSA IT Equipment unless authorized by a CBSA supervisor.
- You are not allowed to enter CBSA offices if there are no CBSA officials present unless you were given permission by a CBSA supervisor.
- In all cases, you must be escorted by a CBSA official when accessing secure CBSA areas unless you were given permission by a CBSA supervisor, and you possess a proper security clearance.
- Under no circumstances may you use CBSA information for personal use, gain or financial benefit for yourself, your relatives or anyone else.
- You must keep in strict confidence all information you obtain about CBSA clients and all other official information to which the public does not have access. This includes information about policies, programs, practices and procedures to which the public does not have official access.
- **Note:** Any person who unlawfully discloses Customs information is guilty of an offence under Section 160 of the Customs Act punishable on summary conviction and liable to a fine of not more than fifty thousand dollars or to imprisonment for a term not exceeding six months or to both that fine and that imprisonment; or is guilty of indictable offence and liable to a fine of not more than five hundred thousand dollars or to imprisonment for a term not exceeding five years or to both that fine and that imprisonment.

**Security of Information Act, Part II of Bill C-36 Entitled the Anti-terrorism Act**

18. (1) Every person with a security clearance given by the Government of Canada commits an offence who, intentionally and without lawful authority, communicates or agrees to communicate, to a foreign entity or to a terrorist group any information that is of a type that the Government of Canada is taking measures to safeguard.

(2) Every person who commits an offence under subsection (1) is guilty of an offence and is liable to imprisonment for a term of not more than 2 years.

**Reporting Security Incidents**

You must immediately notify a CBSA supervisor if you become aware of:

- a security infraction;
- a negligent or criminal act;
- an unsafe or hazardous condition at work;
- an accident or injury to yourself or other individuals;
- a failure on the part of any individuals to observe workplace safety and security standards, rules and procedures; or
- a breach of CBSA information.

You must complete a **Security Incident Report** if requested by a CBSA Official.

Please refer to the security incident **Security Volume - Standard for Security Incident Reporting**.

 Initials:_______

**Misconduct**
You must promptly report to your immediate Supervisor or Manager, or to their Director (if the circumstances warrant) any allegation or suspicion of misconduct, criminal or otherwise, by an employee **(including yourself)** that you are aware of, or have witnessed.

**Attach additional briefing material to support specific security requirements related to functions within the External Service Provider's Section.**

## Take these simple steps to ensure you are applying the proper security safeguards:

- Ensure you keep attractive and sensitive items (including personal items) out of sight. Consider a clean desk best practice.
- Make sure you lock up sensitive information and do not leave it in the open. Our Physical Security organization can assist you with this.
- Ensure that appropriate technology is being used to process sensitive material. Our COMSEC organization can assist you with this.
- Know the sensitivity of information you are handling. If you receive something and are unsure of the sensitivity of the information, contact the originator and ask. Classify documents appropriately.
- Ensure that you have a routine for the disposal of sensitive information. Use an appropriate shredder to destroy protected & classified documents.
- Ensure you have a password on your screensaver and log off at night.
- Ensure you wear your ID card and/or Badge Identifier visibly.
- Ensure you are not taking protected or classified CBSA information home with you at the end of the work day unless you have an approved container for transport and storage of the information. This includes information in paper and electronic format.
- Ensure you report security issues (Form BSF152) to a CBSA supervisor and seek advice from Security.
- Visitors must be escorted at all times.
- Any unfamiliar person encountered within your work space should be politely challenged.
- Place an “Away from the office” security notice in plain view warning individuals not to leave sensitive documents in your workstation.
- Never share your network password.
- Do not install software or hardware without IT authorization.
- You must report to a CBSA supervisor any new criminal conviction(s) and/or police involvement including when charges have been laid that are directly related to you.



Initials:_______

| **Acknowledgement and Contractor Signature Authentication** | |
|---|---|
| I fully understand my responsibilities related to the safeguarding of information and assets as stipulated above and I understand and agree to comply with the above statutory and administrative requirements. I fully understand and agree that failure on my part to comply may result in termination of employment.<br>I, the undersigned attest that the signatures placed on the security screening forms TBS/SCT 330-23 and TBS/SCT 330-60 (if applicable) completed by me and submitted to the Canada Border Services Agency are my own and are true and authentic. | |
| **Name of Individual (external service provider) (print)** | |
| **Title of Individual** | **Company** |
| **Signature** | **Date (yyyy-mm-dd)** |

| **CBSA Briefing Official** | |
|---|---|
| This briefing was provided to the Individual identified above. A Security Screening Certificate and Briefing Form (ref: TBS330-47) was read and signed by the Individual. As the Briefing Official, I have completed Part D of the form TBS/SCT330-47 and I have provided the Individual with a copy of the signed briefing document and a copy of form TBS/SCT330-47. | |
| **Name (print)** | **Region/Branch** |
| **Title of Individual** | |
| **Signature** | **Date (yyyy-mm-dd)** |

**Note:** This signed CBSA Employee Briefing Form for External Service Providers must be returned to the Personnel Security Section in Headquarters along with the signed Security Screening Certificate and Briefing Form TBS/SCT 330-47.




PROTÉGÉ A une fois rempli
PROTECTED A when completed

**SÉANCE D'INFORMATION SUR LA SÉCURITÉ**
**Fournisseurs de services externes**

En vertu de la Politique sur la sécurité du gouvernement, je, soussigné, suis chargé de veiller à ce que vous participiez à une séance d'information sur la sécurité à votre entrée en fonctions à l'Agence des services frontaliers du Canada (ASFC).

Tous les fournisseurs de services externes travaillant pour l'ASFC doivent voir la sécurité comme une responsabilité individuelle importante, et ils doivent donc protéger adéquatement les renseignements de nature délicate (classifiés/protégés) et les biens de valeur.

Vous devez faire le **Module en ligne de sensibilisation à la sécurité** dans les dix jours ouvrables de votre entrée en fonction et respecter toutes les règles de sécurité.

Veuillez prendre note que la personne participant à une séance d'information sur la sécurité donnée par un responsable de l'ASFC doit inscrire ses initiales au bas de chaque page et signer à la dernière page du présent document après avoir eu les renseignements sur la sécurité ou les avoir eus à nouveau.

**Cote de sécurité accordée**
On vous a accordé la cote de sécurité suivante :

- ☐ **Cote secrète**
- ☐ **Cote de fiabilité**
- ☐ **Cote très secrète**

**Responsabilités en matière de sécurité**

- Vous devez assumer la responsabilité et la protection de tous les renseignements et de tous les biens du gouvernement, de tous les immeubles et de tous les biens de valeur qui sont en votre possession ou sous votre contrôle. Si un article est perdu, volé ou endommagé, vous devez immédiatement le signaler à votre superviseur immédiat de l'ASFC ou à un responsable de la sécurité de l'ASFC.
- Vous devez signaler à un superviseur de l'ASFC toute condamnation criminelle et/ou participation policière, notamment lorsque des accusations sont portées et qu'elles sont directement liées à votre personne.
- Si votre carte d'identité est perdue, volée ou endommagée, vous devez alors en aviser votre superviseur immédiat de l'ASFC.
- Lorsque vous quittez l'ASFC, vous devez remettre votre carte d'identité et tous les autres biens appartenant à l'ASFC.
- Vous devez aviser l'ASFC si vous n'êtes plus à l'emploi de l'entreprise avec laquelle l'ASFC a conclu un contrat pour obtenir vos services.

 Initiales : ______

- À moins d'y être autorisé par un responsable de l'ASFC, il vous est interdit d'accéder à tous renseignement de l'ASFC aux bureaux ou dans les bases de données de l'ASFC et de l'examiner.
- Les renseignements de l'ASFC (sur n'importe quel support : papier, CD, clés USB, disquettes, vidéos, etc.) ne peuvent quitter les locaux de l'ASFC à moins que vous obteniez l'autorisation d'un superviseur de l'ASFC et que vous utilisiez un contenant approuvé pour le transport et l'entreposage des renseignements.
- Il vous est interdit d'utiliser l'équipement informatique de l'ASFC à moins qu'un superviseur de l'ASFC ne vous y autorise.
- Vous ne pouvez entrer dans les bureaux de l'ASFC sans la présence d'un responsable de l'ASFC à moins d'obtenir l'autorisation d'un superviseur de l'ASFC.
- Dans tous les cas, vous devez être accompagné d'un représentant de l'ASFC lorsque vous entrez dans un endroit sécurisé de l'ASFC à moins d'obtenir l'autorisation d'un superviseur de l'ASFC et d'avoir une cote de sécurité appropriée.
- Il vous est strictement interdit d'utiliser des renseignements de l'ASFC à des fins personnelles, ou en vue d'en tirer un bénéfice ou un avantage financier pour vous-même, des membres de votre famille ou toute autre personne.
- Vous devez conserver de façon strictement confidentielle tous les renseignements que vous obtenez au sujet des clients de l'ASFC, ainsi que tous les autres renseignements officiels auxquels le public n'a pas accès. Cela comprend les renseignements sur les politiques, les programmes, les pratiques et les procédures auxquels le public n'a pas officiellement accès.

- **Nota :** Toute communication illégale de renseignements douaniers constitue une infraction à l'article 160 de la **Loi sur les douanes** et quiconque commet cette infraction encourt ce qui suit : sur déclaration de culpabilité par procédure sommaire, une amende maximale de cinquante mille dollars et un emprisonnement maximal de six mois, ou l'une de ces peines; par mise en accusation, une amende maximale de cinq cent mille dollars et un emprisonnement maximal de cinq ans, ou l'une de ces peines.

**Loi sur la protection de l'information, partie 2 du projet de loi C-36 intitulé Loi antiterroriste**

18. (1) Commet une infraction le titulaire d'une habilitation de sécurité délivrée par le gouvernement fédéral qui, intentionnellement et sans autorisation légitime, communique des renseignements du type de ceux à l'égard desquels celui-ci prend des mesures de protection à une entité étrangère ou à un groupe terroriste ou accepte de les leur communiquer.
(2) Quiconque commet l'infraction prévue au paragraphe (1) est coupable d'un acte criminel passible d'un emprisonnement maximal de deux ans.

**Signalement des incidents de sécurité**
Vous devez aviser immédiatement un superviseur de l'ASFC si vous constatez ce qui suit :
- une infraction aux règles de la sécurité;
- un acte négligent ou criminel.
- une condition de travail dangereuse ou non sécuritaire;
- un accident ou une blessure à vous-même ou à d'autres personnes;
- le manquement d'un employé au respect des normes, des règles et des procédures de sécurité en milieu de travail. · une fuite de renseignements de l'ASFC.

Vous devez remplir un **Rapport d'incident relatif à la sécurité** si un responsable de l'ASFC vous le demande.

Veuillez-vous référer au volume de sécurité de l'ASFC - Norme pour le signalement des incidents de sécurité.

 Initiales : ______

**Inconduite**
Vous devez signaler sans délai à votre superviseur immédiat ou gestionnaire, ou à leur directeur (si la situation le justifie) toute allégation ou tout soupçon d'inconduite, délit criminel ou autre commis par un employé (**incluant vous-même**) dont vous êtes au courant ou avez été témoin.

**Veuillez joindre les documents d'information supplémentaires à l'appui des règles de sécurité particulières liées aux fonctions au sein de la section du fournisseur de services externes :**

## Faites simplement ce qui suit pour appliquer les mesures de sécurité appropriées

- Assurez-vous de garder les articles attirants et délicats (y compris les articles personnels) hors de la vue. Considérez le rangement de votre bureau comme une pratique exemplaire.
- Veillez à mettre sous clé les renseignements délicats et à ne pas les laisser à la vue. Notre organisme de sécurité matérielle peut aider à ce sujet.
- Assurez-vous que la technologie appropriée est utilisée pour traiter le matériel délicat. Notre organisme de la COMSEC peut vous aider à cet égard.
- Soyez au courant de la classification des renseignements que vous manipulez. Si vous recevez un document et que vous n'êtes pas certain de la classification des renseignements qu'il contient, communiquez avec l'auteur et demandez-lui. Classifiez les documents de manière appropriée.
- Adoptez une routine pour l'élimination des renseignements délicats. Servez-vous d'une déchiqueteuse appropriée pour détruire les documents classifiés et protégés.
- Ayez un mot de passe pour votre économiseur d'écran et fermez votre session le soir.
- Portez votre carte d'identité et/ou votre bande-numéro d'insigne de manière visible.
- Assurez-vous de ne pas apporter à la maison des renseignements de l'ASFC protégés ou classifiés à la fin de la journée de travail à moins d'avoir un contenant approuvé pour le transport et l'entreposage des renseignements. Cela comprend les renseignements sur papier et les renseignements électroniques.
- Signalez les incidents de sécurité (formulaire BSF152) à un superviseur de l'ASFC et sollicitez les conseils de la Sécurité.
- Les visiteurs doivent être accompagnés en tout temps.
- Tous les inconnus rencontrés à votre lieu de travail doivent être questionnés poliment.
- Veuillez placer un avis de la sécurité « À l'extérieur du bureau » bien en vue afin d'avertir les gens de ne pas laisser de documents délicats à votre poste de travail.
- Ne communiquez jamais votre mot de passe du réseau.
- N'installez pas de logiciel ou d'équipement sans l'autorisation de la TI.
- Vous devez signaler à un superviseur de l'ASFC toute condamnation criminelle et/ou participation policière, notamment lorsque des accusations sont portées et qu'elles sont directement liées à votre personne.



Initiales : ______

| Attestation et Authentification de la signature du sous-traitant | |
|---|---|
| Je comprends entièrement mes responsabilités en matière de protection des renseignements et des biens susmentionnées, je comprends et conviens de me conformer à ces exigences légales et administratives. Je comprends entièrement et conviens qu'un manquement de ma part à me conformer à ces exigences pourrait mener au licenciement.<br><br>Je, soussigné(e), certifie que les signatures apposées sur les formulaires d'enquête de sécurité TBS/SCT 330-23 et TBS/SCT 330-60 (s'il y a lieu) remplis par moi et envoyés à l'Agence des services frontaliers du Canada sont les miennes et qu'elles sont véritables et authentiques. | |
| **Nom de la personne (fournisseur de services externe) en caractères d'imprimerie** | |
| **Titre de la personne** | **Enterprise** |
| **Signature** | **Date (aaaa-mm-jj)** |

| Agent de l'ASFC qui a donné la séance | |
|---|---|
| La séance d'information a été donnée à la personne ci-dessus. Cette dernière a lu et signé le Certificat d'enquête de sécurité et profil de sécurité (réf. : TBS/SCT 330-47). À titre de responsable de la séance d'information, j'ai rempli la partie D du formulaire TBS/SCT 330-47 et j'ai remis à la personne une copie du document signé ainsi qu'une copie du formulaire TBS/SCT 330-47. | |
| **Nom (caractères d'imprimerie)** | **Région/Direction générale** |
| **Titre de la personne** | |
| **Signature** | **Date (aaaa-mm-jj)** |

**Nota :** Ce formulaire dûment signé sur la séance d'information sur la sécurité pour les Fournisseurs de services externes de l'ASFC doit être retourné à la section Sécurité du personnel de l'Administration centrale, accompagné du Certificat d'enquête de sécurité et profil de sécurité TBS/SCT 330-47 également signé.

**BSF724F**






# Standard for Security Requirement Checklist (SRCL)

PROTECTION • SERVICE • INTEGRITY

Canada



This standard takes effect on February 2, 2015.

## Purpose:

**1.** The Security Requirement Checklist (SRCL) defines the security requirements for a contract and must accompany all requisitions and related contractual documents, including subcontracts that contain security requirements. The SRCL (Annex A) provides a guide by which the Project Authority can make an initial assessment of the appropriate level of sensitivity of assets involved in the contract and, based on that assessment, can make a reasonable estimation of the general security controls required in order to appropriately protect Government of Canada (GoC) sensitive assets. (Appendix A)

## Background:

**2.** SRCL's were developed to ensure compliance with specific security requirements identified by a federal government department / branch. The SRCL must accompany all requisitions and related contractual documents, including subcontracts that contain security requirements. It does not replace the necessary clauses in the contract but acts as an extension to the specific security requirements.

The SRCL is an integral part of the security in contracting management efforts. Once completed and submitted, the SRCL is used to generate security requirements that are integrated into various documents associated with the contracting process. The SRCL may be accompanied by more detailed direction in the form of a guide that becomes an integral part of the SRCL on submission and is incorporated into the contracting documentation.

The SRCL covers a range of security domains including Physical Security, Information Security, IT Security, COMSEC / INFOSEC and Personnel Security. This is in addition to a number of more specialized controls. Because of the wide range of expertise, it is unlikely that one person holds the accountability across all domains except the Departmental Security Officer (DSO).

## Associated Documents with the SRCL:

**3. Statement of Work (SOW):** The SOW is a formal document that captures and defines the work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client. The SOW usually includes detailed requirements and pricing, with standard regulatory and governance terms and conditions.

**3.1 Contract:** A Contract is an agreement between two or more parties, in this case between the federal government and private industry. This generally involves the private industry undertaking work, to supply goods or provide a service in return for some consideration.







**3.2 Contract Request Summary:** The Contract Request Summary (CRS) is a short brief description of the contract which describes the employer/employee relationship, proposed period of the contract, security classification and project title.

**3.3 Employer/Employee Relationship Checklist:** The Employee/Employer checklist is intended to give you an indication of potential employer/employee relationship(s) within the organization. It is completed and signed by the Project Authority.

**3.4 Statement of Sensitivity (SOS):** The Statement of Sensitivity is often linked to the SRCL when information technology is involved in the contract and maybe affected. A SOS provides a detailed description of the system or application from both an operational perspective and a technical perspective. It also provides a list of the valuable or essential assets forming the IT system with an appreciation of the worth of each asset from a financial or business perspective.

**NOTE:** It is important however, that there is no exception or confusion when it comes to the necessity that the SRCL be accompanied with the SOW. It is recommended that any other documents that are of importance to the SRCL also be included when submitting the SRCL.

## Main Security Domains Covered

### 4.1 PHYSICAL SECURITY (PS):

Physical Security controls are security measures that are designed to deny unauthorized access to facilities, equipment and information and assets and to ensure that all reasonable steps are taken to protect the same from damage or harm. Physical security involves the use of multiple layers of interdependent systems which include but are not limited to: CCTV surveillance, security guards, locks access controls, etc.

### 4.2 COMMUNICATION SECURITY (COMSEC):

COMSEC maintains communication security (Electronic Security). There are four basic components of COMSEC which involves; transmission, physical security, cryptographic equipment and personnel security clearances.

### 4.3 INFORMATION SECURITY (INFOSEC):

To defend information from unauthorized access, use, disclosure, disruption, modification, perusal inspection, recording or destruction.

### 4.4 INFORMATION TECHNOLOGY /ASSESSMENT (IT):

The purpose of Information Technology (IT) security is to ensure that only properly cleared and authorized personnel have access to the equipment and information that they require to process







government sensitive information. It is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.

### 4.5 Personnel Security Clearance (PERSEC):

A personnel security clearance is required for any and all individuals who will have access to sensitive government designated or classified information and or assets. There are essentially three categories of clearance levels which include; Reliability status, Secret and Top Secret.

Facility / information protection is one of the essential subsystems for implementing an effective security program. In order to do so, all components of the SRCL with the assistance of the above mentioned domains, must coordinate all efforts to accomplish this task. (Appendix B)

## Creating an SRCL / SOW:

5. There are a number of key steps that need to be taken to ensure that the SRCL is completed both appropriately and completely. These steps are described below.

6. Government Client / Office of Primary Interest (OPI): **The Client (OPI)** identifies the project through the work to be done (Statement of Work or SOW) and, in consultation with the Project Authority and Contracting Officer, identifies all assets (tangible and intangible) that are implicated in the work.

5.1 The Project Authority Officer generates the Statement of Work in consultation with the Contracting Officer. The information contained in the SOW is then used to complete the SRCL. The levels of sensitivity associated with certain assets uses baselines set by Security. The completed SOW and SRCL are both sent to the Security point of contact **after the Project Authority has signed off the SRCL**.

5.1.1 The SRCL and SOW are sent to the Corporate Physical Security Officer where the Statement of Work meets any one or more of the following criteria:

- The work will take place in conjunction with another country or bloc of countries,
- The work will take place across several regions or the work being conducted in one region is intended to form a baseline for work across several regions, or
- The work is intended to take place with other federal entities operating at the national level.

5.1.2 The SRCL and SOW are sent to the Regional or Headquarters Security Officer where the work described in the Statement of Work does not fall into the above and only implicates that particular region.

5.2 The Security point of contact reviews the SRCL and the SOW, ensuring that the SRCL is fully completed, appropriately reflects the level of sensitivity inferred in the SOW and identifies additional controls to be put in place to ensure that CBSA assets are afforded the appropriate level of protection.







5.2.1 Given that the SRCL covers several domains (Personnel Security, Physical Security, etc.), the SRCL will be reviewed by persons competent in those domains and under the authority of the individuals delegated by the Departmental Security Officer to manage those risks. Coordinating this process is under the control of the Manager Physical Security.

5.3 The reviewed SRCL and any guide defining security controls are communicated back to the Project Authority that reviews them, The security point of contact will seek the initial indication that the Project Authority commits to ensuring that the security controls will be put in place, maintained and monitored throughout the lifecycle of the contract.

5.4 With receipt of the initial commitment, the Organizational Security Authority signs the section on the SRCL, guide and SOW back to the Project Authority. **Once the SRCL has been signed by the Organizational Security Authority, no changes to the SOW may be made. Any changes to the SOW require that the SOW and revised SRCL be reviewed again.**

5.5 The Project Authority submits signed documentation, SOW and any guide to Contracting where they are used to generate the contracting clauses. These will be sent by the Contracting Officer to the Security Officer signing the SRCL as a final confirmation before the contract is let.

5.6 An SRCL is used to assist in determining the security controls to be integrated into any procurement of services. There are cases that do not require the completion of an SRCL. These include the following:

- The procurement of a good where no service (such as when no installation, nor maintenance) is involved;
- Where a contract involving the same work and level of sensitivity is being extended. In these cases, the SRCL from the original contract may be used and a new, while recommended for the purposes of verification, is not needed; and
- Physical Security is currently piloting a project that involves the completion of a master SRCL in cases where identical projects are being run in several locations. In these cases, the Master SRCL may be used *when and only if the Regional or Headquarters Security organization in which the work is being completed or installed* provides written concurrence that the Master SRCL will suffice to meet all security requirements.
- In such cases, CBSA is using form 9200 to confirm that no security elements are present in the contract, therefore, no security screening, site inspection, IT inspections, nor SRCL are required.

## SRCL Delegation Authority:

**6.** The authority to sign as the Organizational Security Officer derives from the authority of the DSO as the Senior Officer responsible for Security risk within the Agency. Within the Agency, there are four positions within the Corporate Security organization and three positions per region established to act as the Organizational Security Officer.



To be delegated to this position, the individual must commit to abide by the program requirements, demonstrate an understanding of these requirements and commit to reporting any attempt or condition that could lead to them being bypassed.

### Online Security Requirements Checklist / Online Industrial Security Services (OLISS):

**7.** This is an electronic service offered and developed by PWGSC Industrial Security Directorate to assist in fast tracking the SRCL process. An application must be completed, approved and signed off by the DSO before processing. The application once it has been approved is electronically forwarded to PWGSC for their records, system up date and registration, which will permit the delegated authority to sign off on SRCLs with full authority. (Appendix D)

### Security Incidents Arising from the Security Clauses

8. The SRCL guide and contracting clauses reflect controls that arise out of the risk management process. This leads to the following:
8.1 The SRCL must reflect an accurate accounting of the levels of sensitivity involved. Deliberately increasing the levels of sensitivity to restrict the competitive field or lowering the level of sensitivity involved to broaden the security field is considered to be inappropriate.

8.2 Any deliberate bypassing of a security control is considered to be a security incident. Where there is a clearly deliberate attempt to bypass controls and allow for unscreened or under-screened persons to gain access to Government of Canada sensitive assets, the incident will be referred for review of Reliability Status or Security Clearance at the discretion of the DSO.

8.3 Attempting to bypass the SRCL process through the use of duplicate SRCLs or by using the results from one project onto another a project is considered to be security incident.

### Revocation of SRCL signing authority:

**9.** The CBSA DSO has the ability and the responsibility to revoke SRCL signing authority to anyone who does not comply with the mentioned directives including, but not limited to the following:

- Not ensuring that all security requirements have been indicated before sign – off
- Falsifying an SRCL or SOW of the security requirements
- Not amending, if required, an SRCL / SOW before contract award
- Not having a proper and up to date signing authority or security clearance
- Lack of appropriate safeguarding methods once the SRCL / SOW have been completed
- Not appropriately completing or reviewing the SRCL / SOW for the advancement of the project and approval stage
- Reducing the level of security for the purpose of advancing the project and approval stage
- Not supplying appropriate documentation relevant to the SRCL / SOW
- Repetitive disregard of CBSA directives when dealing with SRCLs







The DSO has full authority and is responsible for ensuring appropriate remedial actions are taken to address issues regarding policy compliance, allegations of misconduct, suspected criminal activity or security incidents including denying, revoking, or suspending security clearances and reliability status as appropriate.

Annex A – Security Requirements Checklist (SRCL) application with instructions (Form # TBS/SCT 350-103) http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-eng.asp

Annex B – Personnel Security Clearance Applications: Reliability TBS/SCT 330-23E / Secret/Top Secret TBS/SCT 330-60E.

Annex C – Access to and use of the Online Industrial Security Services (OLISS) Registration Form

Annex D - Revocation letter of SRCL Signing Authority

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme liée à la liste de vérification des exigences relatives à la sécurité matérielle (LVERS)

PROTECTION • SERVICE • INTÉGRITÉ





Cette norme entre en vigueur le 2 février 2015.

## Objet

**1.** La liste de vérification des exigences relatives à la sécurité (LVERS) définit les exigences en matière de sécurité à respecter dans le cadre d'un marché et doit accompagner toutes les demandes de soumissions et les documents contractuels qui s'y rattachent, y compris les sous-traitances qui renferment des exigences en matière de sécurité. La LVERS est un guide permettant au responsable du projet de faire une évaluation initiale du niveau approprié de sensibilité des biens liés au contrat et, en se fondant sur cette évaluation, de déterminer de façon raisonnable les mesures générales de sécurité requises pour protéger adéquatement les biens de nature délicate du gouvernement du Canada.
(Voir la LVERS à l'annexe A, en pièce jointe.)

## Contexte

**2.** Les LVERS ont été établies afin d'assurer la conformité à certaines exigences précises de sécurité relevées par un ministère ou une direction générale du gouvernement fédéral. La LVERS doit accompagner les demandes et les documents contractuels connexes, y compris les marchés de sous-traitance contenant des exigences relatives à la sécurité. Elle ne remplace pas les dispositions nécessaires du contrat, mais sert de prolongement aux exigences de sécurité précises.

Les LVERS font partie intégrante de la sécurité dans la gestion des contrats. Une fois remplie et remise, la LVERS sert à produire des exigences de sécurité intégrées dans différents documents liés au processus d'octroi de contrat. La LVERS peut être accompagnée de directives plus détaillées ayant la forme d'un guide qui fait partie intégrante de la LVERS lors de la soumission, et incorporé dans les documents du contrat.

La LVERS porte sur un éventail de domaines de sécurité, y compris la sécurité matérielle, la sécurité de l'information, la sécurité de la TI, COMSEC et INFOSEC, et la sécurité du personnel. Elle s'ajoute à un certain nombre de mesures plus spécialisées. En raison de la diversité des compétences, il est improbable qu'une personne soit responsable de tous les domaines, à l'exception de l'agent de sécurité du ministère (ASM)

## Documents liés aux LVERS :

**3. L'énoncé des travaux** est un document officiel dans lequel sont énoncés et définis les travaux, les produits livrables, le calendrier que doit respecter le fournisseur lorsqu'il doit exécuter un travail précis pour un client. L'énoncé des travaux comprend généralement les exigences détaillées et les prix, ainsi que les dispositions et les conditions normalisées relatives aux règlements et à la gouvernance.

**3.1 Un contrat** est une entente entre deux parties ou plus, dans le cas présent, entre le gouvernement fédéral et l'industrie privée. Généralement, l'entente porte sur des travaux effectués par l'industrie privée, qui doit fournir des biens ou un service moyennant considération.







**3.2 Le sommaire de la demande de marché (SDM)** est une courte description du contrat indiquant la relation entre l'employeur et l'employé, la période visée par le contrat, la cote de sécurité et le titre du projet.

**3.3 La liste de vérification de l'employé et de l'employeur** vise à indiquer les relations possibles entre l'employeur et les employés de l'organisation. La LVERS doit être remplie et signée par le chargé de projet.

**3.4 L'Énoncé de sensibilité (ES)** est souvent lié à la LVERS dans les cas où le contrat englobe de la technologie d'information. L'ES donne une description détaillée du système ou de l'application, et ce, tant sur le plan opérationnel que sur le plan technique. Il fournit aussi la liste des actifs de importants ou essentiels qui font forment le système des TI et une estimation de la valeur de chaque bien sur le plan financier ou commercial.

**NOTA** : Il n'existe aucune exception ni confusion en ce qui a trait à la nécessité d'annexer la LVERS à l'énoncé des travaux. Il est recommandé d'inclure tout document important pour la LVERS lors de la présentation de la LVERS.

## Principaux domaines de sécurité touchés

### 4.1 SÉCURITÉ MATÉRIELLE (SM)

Les contrôles de sécurité matérielle sont des mesures de sécurité conçues pour refuser tout accès non autorisé aux installations, au matériel, à l'information et aux biens et pour veiller à ce que toutes les étapes raisonnables soient suivies pour protéger ces éléments contre tout préjudice. La sécurité matérielle comprend le recours à différentes couches de systèmes interdépendants, notamment : la surveillance par télévision en circuit fermé, les gardes de sécurité, les verrous et les contrôles d'accès et plusieurs autres techniques physiques.

### 4.2 SÉCURITÉ DE LA COMMUNICATION (COMSEC)

La COMSEC maintient la sécurité de la communication (sécurité électronique). La COMSEC compte quatre éléments de base : transmission, sécurité matérielle, matériel cryptographique et autorisation de sécurité du personnel.

### 4.3 SÉCURITÉ DE L'INFORMATION (INFOSEC)

Protection des renseignements contre les consultations, utilisation, divulgation, interruption, modification, lecture, enregistrement ou destruction non autorisés.







## 4.4 ÉVALUATION DES TECHNOLOGIES DE L'INFORMATION (TI)

La sécurité des technologies de l'information (TI) vise à ce que seules les personnes autorisées et ayant subi les vérifications appropriées aient accès au matériel et à l'information dont elles ont besoin pour traiter les renseignements de nature délicate du gouvernement. Il s'agit d'utiliser les ordinateurs et le matériel de télécommunication pour entreposer, récupérer, transmettre et manipuler les données.

## 4.5 Autorisation de sécurité du personnel (SECPER)

Toutes les personnes qui ont accès à des renseignements et/ou à des biens désignés ou classifiés du gouvernement doivent recevoir une autorisation de sécurité. Il existe trois niveaux d'autorisation de sécurité : vérification de la fiabilité, secret et très secret.

La protection des installations et de l'information est un sous-système essentiel pour la mise en œuvre d'un programme de sécurité efficace. Tous les éléments de la LVERS, avec l'aide des domaines indiqués ci-dessus, doivent coordonner leurs efforts pour mener cette tâche à bien. (Voir l'annexe B en pièce jointe).

# Création d'une LVERS ou d'un énoncé des travaux

5. Un certain nombre d'étapes importantes doivent être suivies pour veiller à ce que la LVERS soit entièrement remplie de façon appropriée. Ces étapes sont décrites ci-dessous.

6. Client gouvernemental/Bureau de première responsabilité (BPR) : **Le client (BPR)** indique les projets au moyen des travaux à faire (énoncé des travaux) et, en consultation avec le responsable du projet et l'agent de négociation des contrats, relève tous les biens (tangibles et intangibles) compris dans les travaux.

5.1 L'agent responsable du projet créera l'énoncé des travaux en consultation avec l'agent de négociation des contrats. Les renseignements compris dans l'énoncé des travaux servent ensuite à terminer la LVERS. Le degré de sensibilité lié à certains biens est établi en fonction de lignes directrices établies par la Sécurité. L'énoncé des travaux remplis et la LVERS sont ensuite transmis au point de contact de la Sécurité **lorsque le responsable de projet a approuvé la LVERS**.

5.1.1 La LVERS et l'énoncé des travaux sont transmis à l'agent de sécurité matérielle lorsque l'énoncé des travaux correspond à au moins l'un des critères suivants :

- Les travaux doivent être effectués en collaboration avec un autre pays ou un ensemble de pays.
- Les travaux seront effectués dans plus d'une région, ou seront effectués dans une seule région, puis serviront de fondation pour des travaux dans d'autres régions.
- Les travaux doivent être effectués en collaboration avec d'autres organisations fédérales à l'échelle nationale.



5.1.2 La LVERS et l'énoncé des travaux sont transmis à l'agent de sécurité régional lorsque les travaux décrits dans l'énoncé ne correspondent pas aux critères ci-dessus et ne ciblent qu'une seule région.

5.2 Le point de contact de la sécurité examine la LVERS et l'énoncé des travaux pour veiller à ce que la LVERS soit entièrement remplie et qu'elle corresponde au degré de sensibilité indiqué dans l'énoncé des travaux. Il indique ensuite les mesures de contrôle additionnelles à prendre pour veiller à ce que les biens de l'ASFC obtiennent la protection appropriée.

5.2.1 Comme la LVERS touche plusieurs domaines (PERSEC, SECMAT, etc.), elle doit être examinée par des personnes qui sont compétentes dans ces domaines et sous la supervision de personnes mandatées pour gérer ces risques. Le gestionnaire de la Sécurité matérielle est responsable de la coordination de ce processus.

5.3 La LVERS révisée et le guide définissant les mesures de sécurité sont transmises au responsable du projet, qui les examine. Le point de contact de la sécurité demandera la confirmation que le responsable du projet s'engage à veiller à ce que les mesures de sécurité soient mises en place, maintenues et surveillées tout au long du cycle de vie du contrat.

5.4 Après avoir reçu l'engagement initial, le responsable de la sécurité organisationnelle signe la LVERS, le guide et l'énoncé des travaux et les transmet au responsable du projet. **Lorsque le responsable de la sécurité organisationnelle a signé la LVERS, aucune modification ne peut être apportée à l'énoncé des travaux. Toute modification à l'énoncé des travaux nécessite donc un nouvel examen de l'énoncé et de la nouvelle LVERS.**

5.5 Le responsable du projet présente les documents signés, l'énoncé des travaux et tout guide au service des contrats, qui s'en servira pour rédiger les dispositions du contrat. L'agent de négociation des contrats enverra les documents à l'agent de sécurité responsable de l'autorisation de la LVERS en guise de confirmation définitive avant de conclure le contrat.

5.6 La LVERS est utilisée pour déterminer les contrôles de sécurité qui doivent être intégrés dans tout approvisionnement en services. Dans les cas suivants, la LVERS n'est pas requise :

- L'approvisionnement en biens qui ne comporte pas des services (lorsque le contrat ne comporte pas d'installation ou d'entretien);
- Lorsqu'un contrat comportant le même travail et le même niveau de sensibilité est prolongé. Dans ce cas, la LVERS du contrat initial peut être utilisée. Une nouvelle LVERS n'est pas nécessaire, bien qu'elle soit recommandée aux fins de vérification;
- L'unité de la Sécurité matérielle est à élaborer un projet pilote comportant une LVERS principale pour les cas où des projets identiques sont en cours dans différents emplacements. Dans ces cas, la LVERS principale peut être utilisée *uniquement lorsque l'organisation de sécurité régionale ou de l'Administration centrale dans laquelle les travaux sont effectués* fournit un consentement écrit que la LVERS principale répond à toutes les exigences relatives à la sécurité.
- Dans de tels cas, l'ASFC utilise le formulaire 9200 pour confirmer qu'aucun élément de sécurité n'existe dans le contrat. Par conséquent, aucune vérification de sécurité, inspection de site, inspection des IT ou LVERS n'est requise.



## Délégation des pouvoirs relatifs à la LVERS

**6.** Le pouvoir de signer en tant qu'agent de sécurité organisationnel provient du pouvoir de l'ASM en tant qu'agent principal responsable des risques de sécurité à l'Agence. À l'Agence, quatre postes de la Direction de la sécurité et des normes professionnelles et trois postes par région sont des agents de sécurité organisationnelle.

Pour obtenir ce poste, la personne doit s'engager à respecter les exigences du programme, démontrer qu'elle comprend les exigences et être prête à aviser de toute tentative de contournement des exigences, ou de situation qui pourrait faire en sorte que les exigences ne seront pas respectées.

## Liste de vérification des exigences de sécurité en ligne / Services en direct de sécurité industrielle (SEDSI)

**7.** Il s'agit d'un service électronique offert et conçu par la Direction de la sécurité industrielle de TPSGC pour aider à faire accélérer le processus lié à la LVERS. Avant le traitement, il faut remplir une demande qui doit être approuvée et signée par l'ASM. Une fois approuvée, la demande est envoyée par voie électronique à TPSGC pour les dossiers, la mise à jour des systèmes et l'enregistrement, ce qui permettra au responsable délégué d'autoriser la LVERS. (Voir l'annexe C en pièce jointe)

## Incidents de sécurité découlant des dispositions liées à la sécurité

8. La LVERS, les guides et les dispositions de sécurité représentent les mesures découlant du processus de gestion des risques. Ceci donne ce qui suit :

8.1 La LVERS doit indiquer avec précision les degrés de sensibilité en cause. Il est inapproprié d'augmenter volontairement le degré de sensibilité pour éliminer des concurrents ou de réduire le degré de sensibilité pour élargir le champ de sécurité.

8.2 Tout contournement volontaire d'une mesure de sécurité est un incident de sécurité. Lorsqu'il est clairement démontré qu'une tentative délibérée de contourner les mesures et de permettre à une personne non cotée ou sous-cotée d'avoir accès aux biens de nature délicate du gouvernement du Canada, l'incident doit être signalé à l'ASM aux fins de révision de la cote de fiabilité ou de sécurité.

8.3 Les tentatives de contourner le processus de LVERS au moyen de reproductions ou de l'utilisation des résultats d'un autre projet sont des incidents de sécurité.

## Révocation du pouvoir de signature de la LVERS

**9.** L'ASM de l'ASFC a le devoir et la responsabilité de révoquer le pouvoir de signature de la LVERS de toute personne qui ne respecte pas les directives indiquées, notamment :

- Omission de vérifier que toutes les exigences de sécurité ont été indiquées avant la signature
- Falsification d'une LVERS ou des exigences de sécurité d'un énoncé des travaux
- Omission de modifier, s'il y a lieu, une LVERS ou un énoncé des travaux avant l'octroi du contrat
- Absence d'une attestation ou d'une cote de sécurité adéquate et à jour







- Lacunes en ce qui a trait aux méthodes de protection appropriées une fois la LVERS et l'énoncé des travaux terminés.
- Omission de remplir ou d'examiner de façon appropriée la LVERS ou l'énoncé des travaux avant de faire avancer le projet et de le faire approuver.
- Réduction du niveau de sécurité dans le but de faire avancer le projet et de le faire approuver.
- Omission des documents appropriés et pertinents dans le cadre de la LVERS et de l'énoncé des travaux.
- Manque de respect répété des directives de l'ASFC en ce qui a trait aux LVERS.

L'ASM est chargé de veiller à ce que des mesures correctives appropriées soient prises pour traiter des questions concernant la conformité à la politique, les allégations d'inconduite, les activités criminelles soupçonnées ou les incidents de sécurité, notamment en refusant, en révoquant ou en suspendant les autorisations de sécurité et de fiabilité, selon le cas.

Annexe A - Formulaire et directives de la LVERS (TBS/SCT 350-103) http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-fra.asp

Annexe B - Demandes de vérification de sécurité du personnel : Vérification de la fiabilité (TBS/SCT 330-23F / Secret /Très secret - 330-60E) TBS/SCT 330-60F

Annexe C - L'accès aux Services en direct de sécurité industrielle SEDSI

Annexe D — Lettre de révocation de la part du signataire autorisé de la LVERS

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard Operating Procedures for Security Requirements Checklist

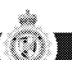
This standard takes effect on February 2, 2015.

PROTECTION • SERVICE • INTEGRITY





TABLE OF CONTENTS



## INTRODUCTION

All regional requisitions that include an element of service provision (i.e. use of personnel), must be accompanied by a Security Requirement Checklist (SRCL) and reviewed by Regional or Headquarters Security to ensure that security requirements are applied and are consistent with the requirements contained in the Policy on Government Security (PGS) of the Treasury Board Secretariat (TBS), the TBS Contracting Policy and the CBSA Contracting Policy (September 1, 2005), issued by the Comptrollership Branch.

SRCLs that have a national impact, such as but not limited to: IT network, facility constructions in more than one region, pilot projects or designs that can impact more than one region, will be reviewed and followed up by HQ Physical Security.

Note: For the purposes of this policy, all Standing Offer call-ups, Local Purchase Orders, Leases, Supply Arrangements, Amendments, etc. are to be considered forms of contracts.

A contract cannot be awarded and work cannot begin until the security requirements (generally defined by the SRCL and any attached Security Guide when dealing with more than one clearance level for the same contract) are met. Once the contract has been awarded, the security requirements must furthermore be maintained throughout the entire duration of the contract.

## PURPOSE

The purpose of this document is to provide the standard operating procedures (SOPs) for the communication and management of SRCLs and SOWs between primary regional stakeholders.

These regional stakeholders are:

- Project Authority/Office of Primary Interest (OPI) client;
- Regional or Headquarters Security; and
- Contracting Authority (CBSA Procurement and/or Public Works and Government Services Canada [PWGSC])

## SCOPE

This document will address the following:

- Overall responsibilities of regional stakeholders; and
- SOPs for the SRCL and SOW processes in which various stakeholders are involved.





## SUMMARY OF RESPONSIBILITIES

### Project Authority (OPI Client)

*Responsible for all matters concerning the scope of work required under a contract.*

- Initiate the SOW and SRCL through consultation with CBSA Procurement when applicable, by:
  - Identifying the security requirements, and
  - Forwarding the SRCL with the SOW to Security for review and sign off;
- Ensure credit check requirement clause, if identified as required by Security, is included in solicitation documents;
- Approve and sign personnel security clearance forms (TBS-330-23) as required, and return forms to Procurement;
- Once clearance has been confirmed, deliver security briefings and have him/her sign the security certificate (TBS-330-47); and
- Ensure security requirements are adhered to throughout duration of the contract.
- Ensure that restrictions are imposed on contractors not to take any pictures of the work site for ulterior motives, such as publicity or posting on the internet. Taking pictures is not authorized.

### Security

*Responsible for validating all security requirements, within the SRCL, for the work required under a contract.*

- Ensure all appropriate security requirements and clauses are appropriate based on the level of sensitivity of identified assets involved in the work and any apparent sensitivity in the work itself;
- Approve and sign off the provided SRCL if appropriate. Note that ONLY employees who have been provided the delegated authority form the DSO can sign off under the security portion.
- Submit SRCL and SOW with identified security requirements to Procurement for processing;
- Review completed personnel security clearance forms received from Procurement and forward to Security and Professional Standards Directorate, Personnel Screening for processing;
- Act as liaison between Procurement and Security and Professional Standards Directorate, Personnel Screening to confirm clearance status for contractor personnel;



- Ensure security briefings have been delivered by the Project Authority; and

- Perform an audit sampling (minimum 10%) of the level of adherence to contract security requirements during contracts.

**Contracting Authority**

*Responsible for all matters relating to procurement and all contractual matters arising from any contracts issued.*

- Include all security requirement clause(s) identified by Security in solicitation documents;

- Prior to contract award, ensure any recommended vendor complies with the security requirements identified in the solicitation documents. This responsibility includes:

    - Verifying with Regional or Headquarters Security whether the identified vendor possesses existing clearance;

    - Providing and forwarding the appropriate security clearance forms to the contractors, if required;

    - Verifying forms completion and forwarding them to the Project Authority/OPI client for signatures. Project Authority (OPI client) will then return the forms to Procurement; and

    - Confirming clearance status with Regional or Headquarters Security.

- Issue notification to Project Authority (OPI client) that contract has been awarded and include a scanned copy of the contract, SRCL, and SOW.

**Signing Authority**

*Responsible for approving and signing the contracting documents.*

- Project authority (OPI Client): all contract documents including the SRCL

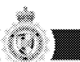
- Regional or Headquarters Security Manager: all security components of contracting documentation (e.g. SRCL and purchase requisition). Note that the Regional or Headquarters Security Manager role may be undertaken by the delegate at Corporate (National) Physical Security under circumstances where the contract falls within the criteria set for national scoping of the contract.

- Procurement Officer: required signature on SRCL

- Contracting Security Authority: required signature on SRCL







## STANDARD OPERATING PROCEDURES

Both SRCL and SOW are required for each acquisition of services and goods where there is a service component that is more than 50% of the total cost. The flow charts below illustrate the communication chain and path of travel the documents are to follow between stakeholders. The SOPs are divided into four (4) contracting categories in which:

1. PWGSC is involved and CBSA Procurement is not;
2. CBSA Procurement is involved and PWGSC is not;
3. Neither PWGSC nor CBSA Procurement are involved; and
4. Both PWGSC and CBSA Procurement are involved.

Please note:

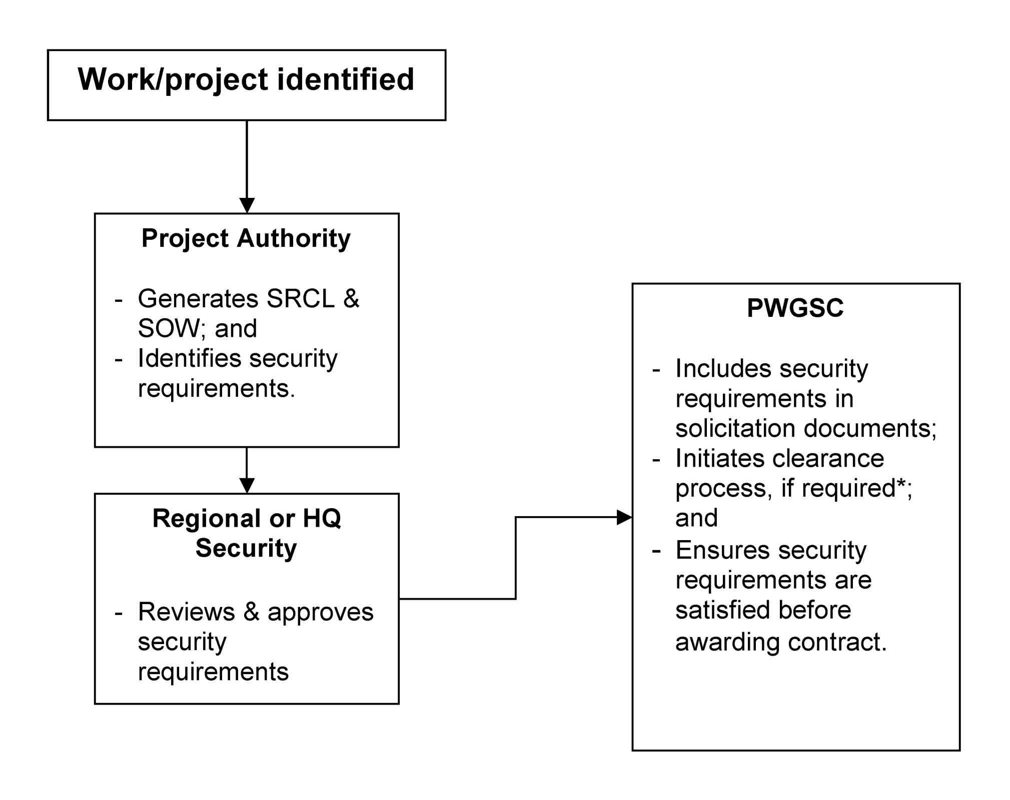
- Until further notice, SRCLs are not required for Section 6 facilities where the contracting is managed by the Air/Marine/Bridge/Tunnel Authority.
- The responsibilities listed in the charts are meant to only provide the general premise of each stakeholder's role and are not comprehensive. For the complete listing of responsibilities, please refer to Summary of Responsibilities.






## SRCL & SOW FLOW: PWGSC INVOLVEMENT

*Where CBSA Procurement is not involved:*




* PWGSC clearance is sufficient for all construction and lease projects in which PWGSC is involved until further notice.

⟶ Denotes hard copy of SRCL (SOW may be sent electronically)

General Categories of Security Requirements:

- Clearance required (at identified level);
- Escort only;
- Clearance and escort required; or
- No security requirements.
- Organizational Facility Clearance










## SRCL & SOW FLOW: PWGSC INVOLVEMENT

(Security Requirement Check List & Statement of Work Flow: Public Works Government Services Canada)

The above flow chart depicts where CBSA Procurement is not involved:

1. The work/project is identified
2. The Project Authority generates the SRCL & SOW and identifies security requirements
3. Regional or HQ Security reviews & approves security requirements
4. PWGSC includes security requirements in solicitation documents, initiates clearance process (if required) and ensures security requirements are satisfied before awarding contract.

Note: In some instances, after step 4 is complete, steps 1 or 3 may be revisited.

Note: PWGSC clearance is sufficient for all construction and lease projects in which PWGSC is involved until further notice.

*Denotes hard copy of SRCL (SOW may be sent electronically)

**The following are General Categories of Security Requirements:**

- Clearance required (at identified level)
- Escort only
- Clearance and escort required
- No security requirements
- Organizational Facility Clearance

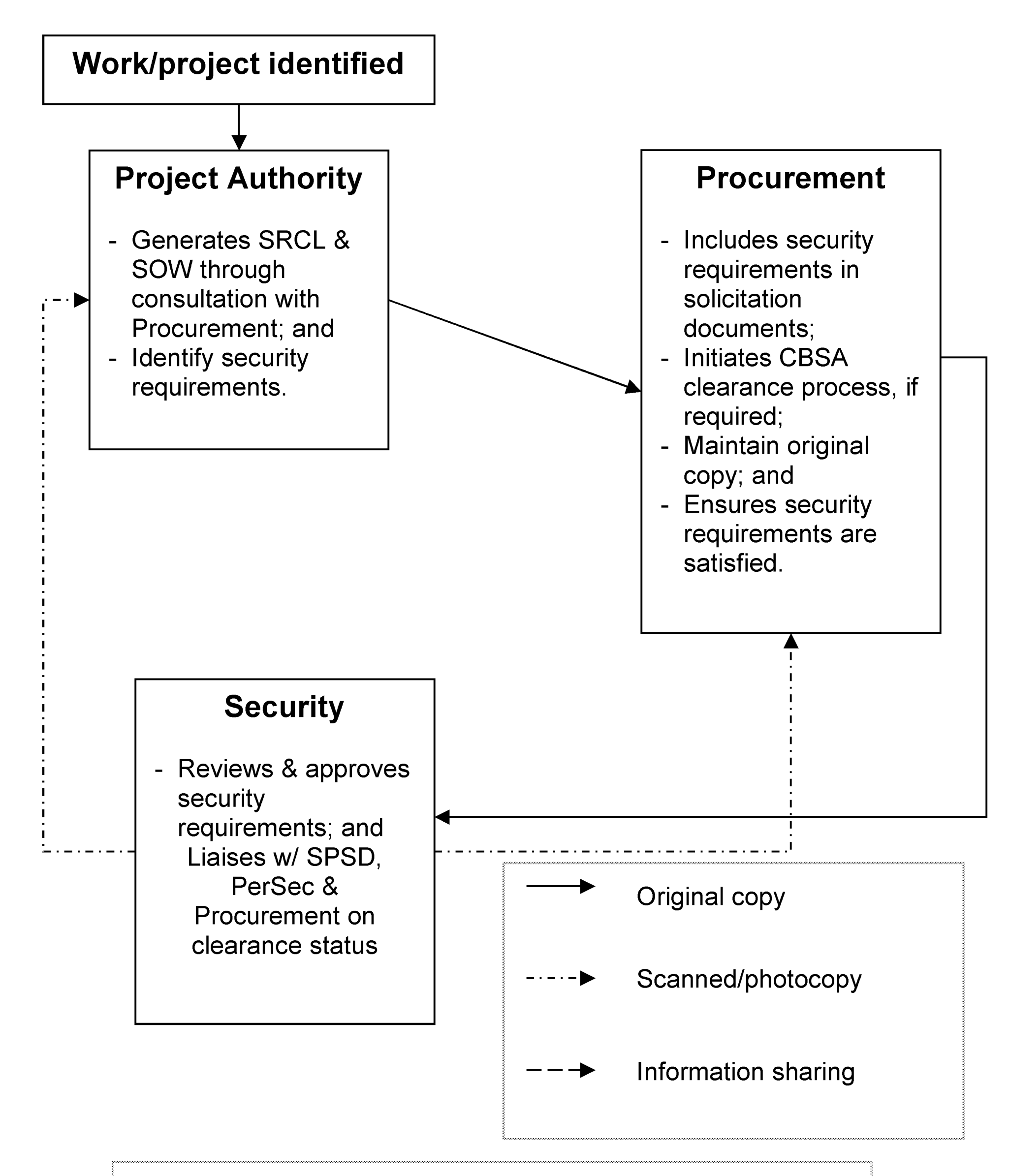






## SOW & SRCL FLOW: CBSA ONLY

*Where PWGSC is not involved:*




General Categories of Security Requirements:

- Clearance required (at identified level);
- Escort only;
- Clearance and escort required; or
- No security requirements.










## SRCL & SOW FLOW: CBSA Only

(Security Requirement Check List & Statement of Work Flow: CBSA only)

The above flow chart depicts where PWGSC (Public Works Government Services Canada) is not involved:

1. The work/project is identified.
2. The Project Authority generates SRCL & SOW through consultation with Procurement and identifies security requirements. Note than an original copy is required.
3. Procurement includes security requirements in solicitation documents, initiates CBSA clearance process, maintains original copies and ensures security requirements are satisfied.
4. Security reviews and approves security requirements and liaises with SPSD (Security and Professional Standards Directorate), PERSEC (Personnel Security) and Procurement on clearance status. In some instances, after this step is complete, steps 2 or 3 may be revisited.

Note: A scanned / photocopy is required for information sharing.

Note: From Steps 2-3 and 3-4, an original copy is needed. From steps 4-1 and 4-3, a scanned / photocopy is needed.

**The following are General Categories of Security Requirements:**

- Clearance required (at identified level)
- Escort only
- Clearance and escort required
- No security requirements

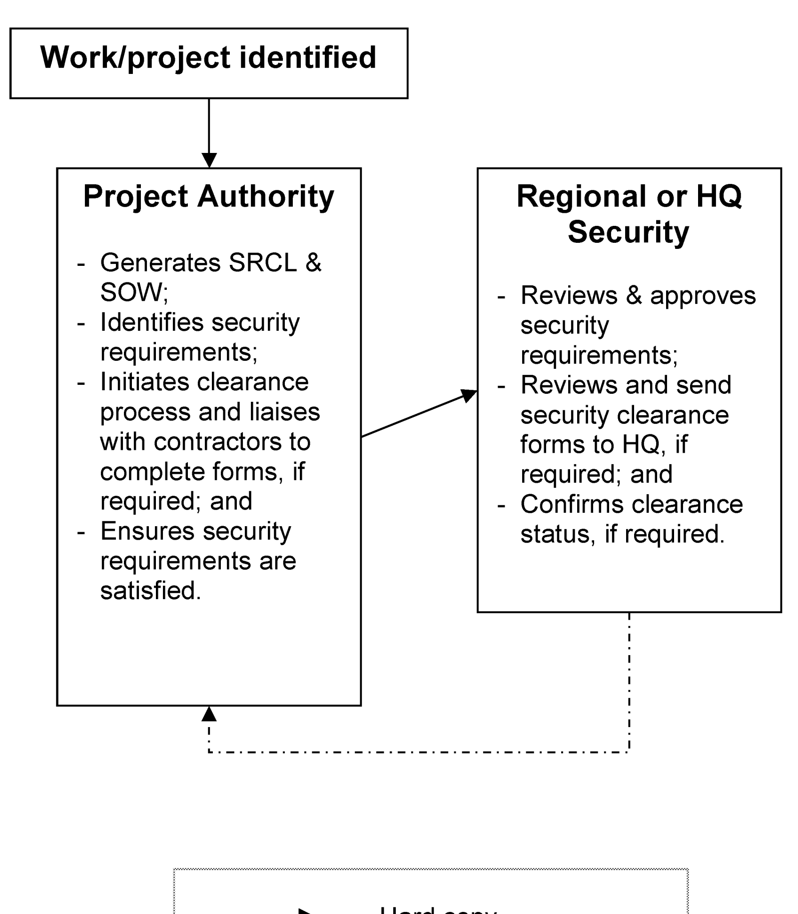






**SOW & SRCL FLOW: CBSA ONLY**

*Where CBSA Procurement is not involved:*




| | |
|---|---|
| ⟶ | Hard copy |
| -·-·-► | Scanned/photocopy |

General Categories of Security Requirements:

- Clearance required (at identified level);
- Escort only;
- Clearance and escort required; or
- No security requirements.



**SRCL & SOW FLOW: CBSA Only**

(Security Requirement Check List & Statement of Work Flow: CBSA only)

The above flow chart depicts where CBSA Procurement is not involved:

1. The work/project is identified.
2. The Project Authority generates the SRCL & SOW, identifies security requirements, initiates clearance process and liaises with contractors to complete forms (if required) and ensures security requirements are satisfied. Note that a hard copy is required.
3. Regional or HQ Security reviews and approves security requirements, reviews and sends security clearance forms to HQ (if required) and confirms clearance status (if required). Note than a scanned / photocopy is required from steps 3-2.

**The following are General Categories of Security Requirements:**

- Clearance required (at identified level)
- Escort only
- Clearance and escort required
- No security requirements



## APPENDIX A: SECURITY CLAUSE FORM

**This annex is reserved for the anticipated PWGSC standard security in contracting clauses which are currently being reviewed at PWGSC policy level.**

## APPENDIX B: Security Requirements Checklist form

http://publiservice.tbs-sct.gc.ca/tbsf-fsct/350-103-eng.asp

## APPENDIX C: Classification Guide

## CLASSIFICATION GUIDE — INFORMATION AND RECORDS

Sanitization of Drawings:

It is critical for the consultants to understand the importance of ensuring that sensitive documents and drawings are properly handled, stored, transported, transmitted and destroyed. It is important that consultants (first) understand that the documents are sensitive and are not to be released without the authorization of the Project Authority and (second) that the level of sensitivity may require that specific controls are put in place. The project authority will consult with security with respect to identifying the level of sensitivity involved.

It is critical that all construction drawings are sanitized prior to being issued to contractors without the appropriate clearance.

Sanitized drawings must meet the following criteria:

1. Construction drawings will not contain a key plan or partial key plan either in the drawing margin or on the drawing showing the complex or site,
2. Construction drawings will not show Government logos, names, or site addresses
3. Rooms must be identified by number, not names. A separate coded list of room numbers associated to sensitive information and descriptors must be developed and regularly up-dated as changes are made. This list must be marked Protected 'B'.
4. Security system information and information regarding security controls (e.g. electronic access control information, intrusion detection information), must be placed on separate layers of construction drawings for ease of printing and distribution and shall not be given in whole or in part to unscreened persons.
5. As-built drawings must not contain any information deemed sensitive as outlined above. It should be noted that where the room design is the primary form of protection of sensitive assets, the room design is considered to also be a security control.
6. Drawings that have been sanitized should be marked "Not to be copied unless authorized by (insert name of project authority) / Controlled Distribution"

**NOTES:**

1. The type of information that would be generated as part of the project that would be considered sensitive includes:

- Vulnerabilities of systems, processes, procedures or equipment, leading to the causing of injury, serious injury or extremely grave injury,







- All Safeguards, (e.g. Physical, Personnel, ITS, Administrative), that mitigate vulnerabilities and/or identified threats,
- Assets/Operations (e.g. Valuable/sensitive equipment/operations and their associated location, weapons and their location, narcotics and their location, etc.), knowledge of which can cause injury, serious injury or extremely grave injury,
- Threats (e.g. Theft, vandalism, demonstrations, bomb threats, robbery, etc.) and associated adversaries causing injury, serious injury and extremely grave injury.

2. It is the responsibility of the originator of the document to determine if the document is sensitive. This determination must take into account and respect baseline security requirements communicated by Security.

Note: For purposes of this project, the project authority will assist any of the project consultants with the appropriate marking of documents that they create. It is critical that the consultants review this document so they understand the type of information that needs to be protected. If in doubt, the consultants should ask the project authority if it is important that the consultants do not mistakenly transmit or transport sensitive documents.

3. In some instances, documents are sensitive as an aggregate report but some of the individual documents making up the report are a lesser sensitivity. These individual documents can be communicated as per their individual level of sensitivity but the Project Authority or distributor of the document must take all reasonable steps to ensure that they are not distributed in such a way as that they could be reassembled.

4. When transmitting sensitive documents, refer to RCMP Guide G1 -009 Transport and Transmittal of Protected and Classified Information.

All persons being given access to sensitive assets must possess both a valid security screening (granted at a level commensurate to the level of sensitivity involved) and a need to have access in order to complete the work (need to know). It is incumbent on the Project Authority to ensure that any person (including non-employees) that are being given access to these assets (including documents) meet this criteria *and* are made aware of any controls that are to be maintained at all times. The Project Authority must also ensure that the security controls remain in force throughout the full period of the contract.

## Retention of Sensitive Documents

Sensitive documents shall be retained for a period of time as determined by the project authority. Sensitive documents must be properly handled and stored until the legal, historical or archival value has expired. At this time, the sensitive documents can then be destroyed by an approved method. If documents are downgraded to non-sensitive information by the project team, then they can be disposed of as normal waste.







Sensitive documents must be returned upon demand by the Agency. Where such documents are being retained in terms of documentation of proof of work, the Agency must provide a suitable indicator that the work was completed to the contractor if taking this step. This will be addressed on a case-by-case basis.

While under the control of Contractors and Consultants, sensitive documents must be stored in an approved manner and only accessible by personnel with the appropriate up-to-date personnel security clearance. If it is suspected that sensitive documents have been compromised the project authority should be contacted immediately.

## Destruction of Protected Information off Site

The security requirements pertaining to commercial destruction services apply to more than just the size of the particle. They apply to the entire process for the destruction of sensitive information and includes everything from procedures for handling and storing the information to procedures for disposing of the waste, the facility responsible for destruction and its personnel.

Protected information must never be stored, even temporarily; at commercial destruction facilities unless the facility has a PWGSC-PWGSC ISP approved Document Safeguarding Capability.

If commercial destruction companies provide containers for the collection and/or temporary storage of Protected documents awaiting collection, contact PWGSC-PWGSC ISP to verify container suitability. Containers with open slots should never be used for the temporary storage of Protective information. Open slot containers may be used for collection and transportation to the destruction site provided they are not used as storage containers and are not left unattended.

If using off-site destruction facilities, contact the PWGSC-PWGSC ISP for guidance on transporting Protected material to that facility.

Personnel at Commercial destruction facilities should not be asked to sort documents. To ensure the protection of sensitive information, documents should either be sorted by appropriately cleared departmental personnel before entering the destruction process, or simply destroyed together by a destruction process that has a security rating equivalent to that of the information having the highest sensitivity. In addition, sorting before destruction involves unnecessary handling of sensitive material and increases the security risk.



## Mobile Destruction Services

Information should be destroyed as close to the origin as possible and preferably, within a controlled and isolated area. It is preferred public streets and lanes or alleys not be used for the destruction of sensitive information.

Security clearances are rarely given to individual employees of mobile shredding companies due to the instability of this workforce and the difficulties in keeping the clearances current. The destruction of sensitive information should be supervised by an appropriately cleared representative(s) of the Agency.

## Approved Destruction Equipment

### Destruction by Shredding, Disintegrating and Grinding of Protected A and B information

Applies to:

Hard-disc drive (HDD)
Floppy disks
CD and DVD
USB Thumb Drives
PDAs including BlackBerrys and other flash memory (EEPROM) devices

If the Consultants want to purchase approved office type shedders for the destruction of sensitive documents, contact PWGSC ISP to purchase approved equipment through their office. PWGSC ISP also has a list of approved bulk destruction facilities if this method of destruction is chosen.

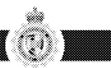
### Destruction by Shredding of Protected A and B information

Applies to: Paper documents

If Consultants want to purchase approved office type shedders for the destruction of sensitive documents, contact the PWGSC ISP and purchase equipment through their office. PWGSC ISP also has a list of approved bulk destruction facilities if this method of destruction is chosen.







# GUIDELINES FOR THE TRACKING OF SENSITIVE INFORMATION DURING HANDLING, DISTRIBUTION AND DESTRUCTION

## General

This document outlines guidelines for the tracking during handling, distribution and destruction of sensitive information for use during the design and construction of Agency projects. The intent is to track the total number of drawings, specifications and CDs.

It is expected that much, if not all of the sensitive information associated with this project will be designated Protected *'A'* or Protected 'B'. If other documents of a higher classification level are received or generated, contact Security for guidance.

## Procedures for Handling, Distributing and Destroying Protected Information

All drawings and associated documents will originate with the prime consultant. Original documents will be sent to the reproduction consultant for printing the required number of sets. Once printed, the sets are to be logged prior to distribution. If extra sets are required once the original order has been fulfilled, these sets will be logged in the same manner indicating who received the set(s).

All copies produced by the reproduction company that are either unusable, are test samples, or just mistakes etc. are to be destroyed. The cover sheet of each set of drawings will be stamped with a text block.

Sample Block

Drawing Distribution

Set: ______ of ______

Company: ________________

Received
SEP 19 2008
MUC Ottawa

Date out:

Date Returned: ____________

Left graphic shows an image of a **Sample Block** with the following information:

Drawing Distribution
Set: *blank* of *blank*
Company: *blank*
Date out:
Date returned:







As consultants and users receive their sets of documents, they will log each set received and who it was distributed to within their organization. Each sensitive document(s) must be cross-referenced as to when it was received / created and when it was destroyed and recorded in a log and available for inspection by the project authority. All undestroyed sensitive documents must be returned to the Project Authority unless they are part of the Consultant's official records. See section on Retention of Sensitive documents. The following information is to be included on the log:

a) Item no. or file no.

b) Date and time document received and where it came from

c) Received by (print name and initial)

d) Title of document

e) Document description (e.g. drawing. titles, sketch titles etc.)

f) If information destroyed, who was notified and who destroyed or supervised destruction

g) If information picked up, by whom and when (time & date).

Drawings shall not be removed from the site by contractors. Contractors will sign out drawings when required and return them to the designated (insert name of project authority) representative at the end of each work day. There is no requirement for Contractors to retain copies of drawings or documents once their portion of the work is completed.

The distribution of information/drawings at meetings will be officially recorded, (i.e. # of # and date). The distribution of these documents will be noted on the sign-in sheets and any left over documents not distributed will be immediately recorded as destroyed as outlined in this guideline. Both the distributor and the recipient will be responsible to ensure these documents are logged in their own system.

Protected information must be identified and treated as sensitive until declassified or destroyed. When destroying Protected information, appropriate measures must be taken to ensure the security of the information during collection, storage (including temporary storage), transport or transmittal and handling during destruction

Protected information shall, pending destruction, be kept separate from unclassified or non-protected information awaiting destruction.





Protected information with no historical or archival value for which the retention period has expired, must be promptly destroyed including surplus copies, draft copies and waste. All Protected information when destroyed, is to be logged. Protected information must not be disposed of through a federal, provincial, municipal or private recycling program unless properly destroyed in an approved manner prior to recycling.

Before any destruction of documents occurs, written consent of the project authority or designate must be obtained.

Anyone who destroys or supervises the destruction of Protected information is security screened commensurate with the highest level of information being destroyed.

Out of date or rejected Protected documents including drawings are still considered Protected even though they are no longer relevant. They must be destroyed in the approved manner and are not to be considered as non-sensitive information unless they are downgraded to non-sensitive by the project team security personnel.



# APPENDIX D: IT and Physical Security Guidelines

## Security requirement for processing protected information on computer systems

Non-sensitive information can be transmitted over the corporate system and the Internet.

Protected information should be processed on a standalone computer, with no connectivity to any network, including the Internet.

Connection of the computer to a corporate system cannot be authorized unless the corporate network is evaluated by PWGSC ISP and the network meets Government of Canada requirements. Protected information should be encrypted before being ported from a standalone computer to a network-connected computer for transmission.

Protected information must be encrypted in transit with product validated under the Common Criteria scheme http://www.commoncriteriaportal.org/products/ or as specified by the CBSA security authorities.

The encryption product must use encryption algorithm approved by CSEC for the protection of protected information https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsa11e-eng_0.pdf or as specified by the CBSA security authorities.

Encryption password\passphrase must be treated as Protected information and exchanged securely, using a different communication mean than the encrypted message (i.e. telephone land line)

When no longer required, protected information must be deleted with secure deletion utilities that are validated under the Common Criteria or the storage media is disposed of according to government standards or as specified by the CBSA security authorities.

Users must receive regular Security Awareness Briefings to be reminded of corporate security policies and practices.

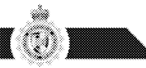
Breach or suspected breach of the security of computer systems used to process protected information must be reported to CBSA corporate security and PWGSC ISP immediately.

A standalone computer with a direct Internet connection may be used:

• Computer operating system implements the security recommendation of the CSEC COTS security guidance 'Summary of secure use of operating systems" CSG-1O/S https://www.cse-cst.gc.ca/en/publication/csg-10

• Critical security updates are monitored and implemented promptly for the operating system and applications.

• Malware protection is implemented and anti-Malware data files are updated on a daily basis.



• A hardware router\firewall is implemented between the computer and the Internet and provides Network Address Translation (NAT).

• Browser is configured not to allow unsigned mobile code (i.e. ActiveX) to run.

• Remote control utilities (Remote Desktop Connection, Remote Assistance, PC anywhere) are not enabled.

• A software firewall (built-in the operating system or as an add-on product) is enabled.

• Corporate policy prohibits users from downloading or using unauthorized software.

• A configuration management and change management process is in place to locally authorize software installation.

• User accounts have only limited system access privileges.

• Protected Information is saved on removable media that is stored separately when not in use in accordance with Physical Security Requirements for the applicable level of protected information (for example SECRET information will require much more Physical Security controls than PROTECTED B information and less for PROTECTED A).

• CLASSIFIED SECRET information must never be viewed or stored on IT systems (i.e. network, laptop, phones, standalone workstations, USB keys, etc...) that doesn't meet the CBSA's Physical Security, Information Security and IT Security Requirements for CLASSIFIED SECRET systems.

• CLASSIFIED TOP SECRET information must never be viewed or stored on IT systems (i.e. network, laptop, phones, standalone workstations, USB keys, etc...) as it is prohibited for security reasons.



PHYSICAL SECURITY REQUIREMENTS

There are a number of known contributing factors to the recommendations provided for this Interim Contract Security Procedures.

The following assumptions are to be considered:

- Depending on the size of the project, there may or may not be on-site offices/trailers for Construction Management and sub-trades. Generally the Construction Manager/General Contractor will have an office or trailer for most projects.

- Most sub-trades require full architectural, structural, mechanical and electrical drawings in order to coordinate their work, and to complete daily layouts for their crews to continue with a productive installation. These drawings and specifications usually can be found on an open floor, on top of a makeshift table. Anyone can wander in and view the information. They generally remain in the working areas overnight when there is no one present.

- If these articles are locked up for the night, it is usually just deposited in a job box (usually nothing more than a plywood box with a drop lid and secured with a chain and keyed lock or combination lock, all off the shelf style with no specific security design.

- Construction sites are continuously being searched. Theft of materials, break and enter into job boxes with theft of tools is a possible occurrence on many job sites.

- Very few sites have external fenced barriers or after hour patrols unless specifically ordered in the contract.

With these assumptions in mind the following requirements for physical security need to be considered. Requirements are divided into two parts, the office environment where design processes will be conducted, and the job site, where drawings are used to build the deliverables.







PERSONNEL SCREENING

- Architect, engineering, and Construction Management teams actually working on the project must have the appropriate screening or clearances. For these interim procedures, screening must be to a minimum of Reliability Status.

- Senior company officials and on-site supervisors must meet the same requirements as Architects as they will have access to complete sets of plans and specifications.

- Journeymen - workers - mechanics will not be required to have a Reliability check done, but they must be supervised at all times, and escorted in completed spaces, occupied spaces, or sensitive areas as designated by CBSA. They are not to have access to sensitive assets.

OFFICE

The office buildings and specific office spaces where contract personnel will be working must implement layers of security similar to that prescribed in Federal Government baseline Standards (i.e. Policy on Government Security) and as the case warrants, applicable extracts from the RCMP Guidelines (G1-025). PWGSC ISP will provide references to standards that must be met by them under the industrial security program.

1. Perimeter of the office in question must be secured after hours. Doors must have at a minimum a locking latch set and an auxiliary dead bolt.

2. Office spaces must be electronically monitored or the drawings and specifications must be secured within a room designed for security, similar to CBSA secure room standards, or within a safe, shell, or cabinet similar to the approved cabinets used by the Federal Government (with a combination dial).

3. The office must be able to accommodate sub-trade viewing of plans and specifications for review of projects for tendering purposes.

4. Drawings must be closely controlled as per the instruction provided in the tendering process.

5. Drawings and specifications will refer to rooms by room number only. Names or function of the rooms are not to be used unless the end user is cleared to see such information.

6. Drawings and specifications for security devices, CCTV camera, and digital recorders MUST be sanitized where unclear users will need access to the drawings. Ideally, rough in of wiring or cabling for such devices will be done on the base work contract while a separate tender for supply and install of the devices to only properly cleared contractors will be used. Where








separate tendering is not feasible, then specifics on such devices and their locations should only be released to the successful bidder. This would rely on unit pricing for the tender with actual specs and layout sketches provided after the contract award.

## CONSTRUCTION SITE

Drawings and specifications must be rolled up daily and deposited into a secure lockup within the office of the General Contractor/Construction Manager (GC/GM).

- The GC/CM site office must be large enough to accommodate secure cabinets in which all sub-trades will lock-up their drawings and specifications. Combinations or key control for these cabinets will remain the responsibility of the GC / CM.

- The GC / CM will be responsible to ensure that all drawings and specs are secured after hours.

- The GM /CM office or trailer will be alarmed with monitored door contacts and motion sensor that will activate a police or security service response. CBSA Regional Security and the Project Authority must be notified of any such alarm condition within 24 Hrs.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Procédures normales d'exploitation (PNE) concernant la liste de vérification des exigences relatives à la sécurité

Cette norme entre en vigueur le 2 février 2015.

PROTECTION • SERVICE • INTÉGRITÉ





TABLE DES MATIÈRES –PNE CONCERNANT LA LVERS







Cette norme entre en vigueur le 2 février 2015.

## INTRODUCTION

Toutes les demandes d'achat des régions qui comprennent un élément de prestation du service (c.-à-d. l'utilisation de personnel) doivent être accompagnées d'une liste de vérification des exigences relatives à la sécurité (LVERS) et doivent être revues par la Sécurité régionale ou la Sécurité de l'Administration centrale (AC) afin de s'assurer que les exigences de sécurité sont appliquées et qu'elles sont conformes aux exigences de la Politique sur la sécurité du gouvernement du Secrétariat du Conseil du Trésor (SCT), de la Politique sur les marchés du SCT et de la Politique sur les marchés de l'ASFC (1er septembre 2005), qui a été diffusée par la Direction générale du contrôle.

Feront l'objet d'un examen et d'un suivi par la Sécurité matérielle de l'AC, les LVERS qui ont une portée nationale, notamment, mais non exclusivement le réseau des TI, la construction d'installations dans plus d'une région, les conceptions ou projets pilotes pouvant toucher plus d'une région.

Remarque **:** Aux fins de l'application de la présente politique, toutes les commandes subséquentes à une offre à commande, les commandes d'achat local, les baux, les arrangements en matière d'approvisionnement, les modifications, etc. sont des formes de marché.

On ne peut attribuer un marché et le travail ne peut commencer avant que ne soient satisfaites les exigences de sécurité (généralement définies dans la LVERS et tout guide relatif à la sécurité qui y est joint lorsque plus d'un niveau d'autorisation de sécurité est requis pour le même marché). Lorsque le marché est attribué, les exigences de sécurité doivent par ailleurs être maintenues pendant toute la durée du marché.

## BUT

Le présent document vise à fournir des PNE pour la communication et la gestion des LVERS et des énoncés des travaux entre les principaux intervenants régionaux.

Ces intervenants régionaux sont :

- Le chargé de projet/le client du Bureau de première responsabilité (BPR);
- La Sécurité régionale ou la Sécurité de l'Administration centrale;
- L'autorité contractante (Approvisionnements de l'ASFC et/ou Travaux publics et Services gouvernementaux Canada [TPSGC])

## PORTÉE

Le présent document traite :

- des responsabilités générales des intervenants régionaux;







- des PNE pour les processus relatifs aux LVERS et aux énoncés des travaux auxquels participent divers intervenants.

- **RÉSUMÉ DES RESPONSABILITÉS**

**Chargé de projet (BPR client)**

*Il est responsable de toutes les questions concernant la portée des travaux à exécuter dans le cadre d'un marché.*

- Il établit l'énoncé des travaux et la LVERS en consultant les Approvisionnements de l'ASFC, s'il y a lieu, et en :
  - déterminant les exigences de sécurité;
  - transmettant la LVERS avec l'énoncé des travaux à la Sécurité aux fins d'examen et de signature.
- Il veille à ce que la disposition de vérification du crédit, si elle est définie comme étant une exigence par la Sécurité, se trouve dans les documents d'invitation à soumissionner;
- Il approuve et signe les formulaires d'autorisation de sécurité du personnel (SCT-330-23) au besoin, et il les retourne aux Approvisionnements de l'ASFC;
- Lorsque l'autorisation de sécurité est confirmée, il donne à l'entrepreneur une séance d'information sur la sécurité et lui fait signer le certificat de sécurité (SCT-330-47);
- Il s'assure que les exigences de sécurité sont respectées pendant toute la durée du marché.
- Il veille à ce que des restrictions soient imposées aux entrepreneurs leur interdisant de prendre des photographies du lieu où se déroulent les travaux pour des motifs cachés, tels que de la publicité ou la publication sur Internet. La prise de photographies est interdite.

**Sécurité**

*Elle est responsable de valider toutes les exigences de sécurité figurant sur la LVERS pour le travail à exécuter dans le cadre du marché.*

- Elle veille à ce que toutes les dispositions et les exigences de sécurité soient adaptées au niveau de sensibilité des biens identifiés qui entrent en jeu dans les travaux, et à toute sensibilité apparente dans le travail lui-même;







- Elle approuve et signe la LVERS fournie, s'il y a lieu. Veuillez noter que SEULS les employés ayant reçu des pouvoirs délégués de l'agent de sécurité du ministère (ASM) peuvent signer la partie sur la sécurité.
- Elle envoie la LVERS et l'énoncé des travaux avec les exigences de sécurité établies aux Approvisionnements aux fins de traitement.
- Elle examine les formulaires d'autorisation de sécurité du personnel dûment remplis que lui envoient les Approvisionnements et elle les transmet aux Enquêtes de sécurité sur le personnel de la Direction de la sécurité et des normes professionnelles aux fins de traitement.
- Elle assure la liaison entre les Approvisionnements et les Enquêtes de sécurité sur le personnel de la Direction de la sécurité et des normes professionnelles afin de confirmer l'état de l'autorisation de sécurité pour les membres du personnel de l'entrepreneur.
- Elle s'assure que les séances d'information sur la sécurité ont été données par le chargé de projet.
- Elle fait une vérification par échantillonnage (au moins 10 %) du degré de conformité aux exigences de sécurité des marchés pendant la durée de ceux-ci.

## Autorité contractante

*Elle est responsable de toutes les questions relatives à l'approvisionnement et au marché pour tout marché établi.*

- Elle inclut dans les documents d'invitation à soumissionner toutes les dispositions relatives aux exigences de sécurité établies par la Sécurité.
- Avant l'attribution du marché, elle s'assure que tout fournisseur recommandé se conforme aux exigences de sécurité indiquées dans les documents d'invitation à soumissionner. Cette responsabilité comprend ce qui suit :
    - vérifier auprès de la Sécurité régionale ou de la Sécurité de l'Administration centrale si le fournisseur retenu possède une autorisation de sécurité;
    - envoyer les formulaires d'autorisation de sécurité appropriés aux entrepreneurs, s'il y a lieu;
    - vérifier que les formulaires ont été remplis et les acheminer au chargé de projet/BPR client aux fins de signature. Le chargé de projet (BPR client) les retourne ensuite aux Approvisionnements;
    - confirmer l'état de l'autorisation de sécurité auprès de la Sécurité régionale ou de la Sécurité de l'Administration centrale.







- Elle envoie un avis au chargé de projet (BPR client) lui indiquant que le marché a été attribué et inclut une copie numérisée du marché, de la LVERS et de l'énoncé des travaux.

## Signataire autorisé

*Il est responsable d'approuver et de signer les documents relatifs à la passation des marchés.*

- Chargé de projet (BPR client) : tous les documents relatifs aux marchés, y compris la LVERS.
- Gestionnaire régional de la sécurité ou gestionnaire de la sécurité à l'AC : toutes les composantes de sécurité des documents relatifs à la passation des marchés (p. ex. la LVERS et la demande d'achat). Remarque : une personne désignée de la Sécurité matérielle de l'Agence (nationale) peut assumer le rôle de gestionnaire régional de la sécurité ou de gestionnaire de la sécurité à l'AC lorsque le marché correspond aux critères établis pour les marchés de portée nationale.
- Agent d'approvisionnement : signature requise sur la LVERS.
- Autorité responsable de la sécurité relative à la passation de marchés : signature requise sur la LVERS.







## PROCÉDURES NORMALES D'EXPLOITATION

La LVERS et l'énoncé des travaux sont requis pour chaque acquisition de biens et de services où une composante de service compte pour plus de 50 % du coût total. Les diagrammes ci-dessous illustrent la chaîne de communication que doivent suivre les documents entre les intervenants. Les PNE se divisent en quatre (4) catégories de passation de marchés auxquelles :

1) TPSGC participe et les Approvisionnements de l'ASFC ne participent pas;

2) Les Approvisionnements de l'ASFC participent et TPSGC ne participe pas;

3) Ni TPSGC, ni les Approvisionnements de l'ASFC ne participent;

4) TPSGC et les Approvisionnements de l'ASFC participent.

Remarque

- Jusqu'à nouvel ordre, les LVERS ne sont pas requises pour les installations aux termes de l'article 6 si la passation du marché est gérée par l'autorité aéroportuaire, maritime, du pont ou du tunnel.

- Les responsabilités énumérées dans les diagrammes ne visent qu'à donner une idée générale du rôle de chaque intervenant et la liste n'est pas exhaustive. Pour la liste complète des responsabilités, veuillez consulter le résumé des responsabilités.

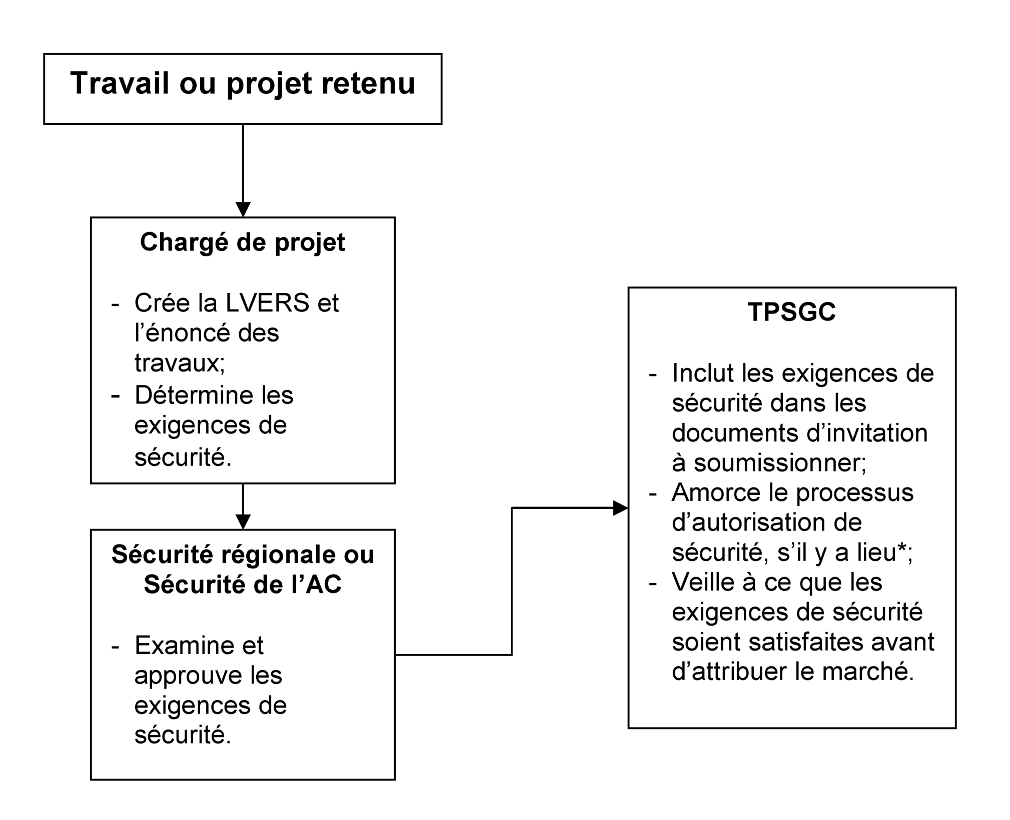






**ACTIVITÉS RELATIVES À LA LVERS ET À L'ÉNONCÉ DES TRAVAUX : PARTICIPATION DE TPSGC**

*Lorsque les Approvisionnements de l'ASFC ne participent pas*




*Jusqu'à nouvel ordre, l'autorisation de sécurité de TPSGC est suffisante pour tous les projets de construction et de location auxquels participe TPSGC.

→ Copie papier de la LVERS (l'énoncé des travaux peut être transmis par voie électronique)

Catégories générales d'exigences de sécurité :

- Autorisation de sécurité requise (au niveau établi);
- Accompagnateur seulement;
- Autorisation de sécurité et accompagnateur requis;
- Aucune exigence de sécurité.
- Cote de sécurité d'installation de l'organisation.







## ACTIVITÉS RELATIVES À LA LVERS ET À L'ÉNONCÉ DES TRAVAUX : PARTICIPATION DE TPSGC

(Lorsque les Approvisionnements de l'ASFC ne participent pas)

Le diagramme ci-dessus démontre les activités relatives à la LVERS et à l'énoncé des travaux lorsque les approvisionnements de l'ASFC ne participent pas:

1. Le travail ou projet est retenu
2. Le chargé de projet crée la LVERS et l'énoncé des travaux et détermine les exigences de sécurité
3. La sécurité régionale ou sécurité de l'AC examine et approuve les exigences de sécurité
4. La TPSGC inclut les exigences de sécurité dans les documents d'invitation à soumissionner, amorce le processus d'autorisation de sécurité (s'il y a lieu) et veille à ce que les exigences de sécurité soient satisfaites avant d'attribuer le marché.

Nota: Dans certains cas, après que la 4e étape soit complétée, les étapes 1 ou 3 peuvent être revisitées.

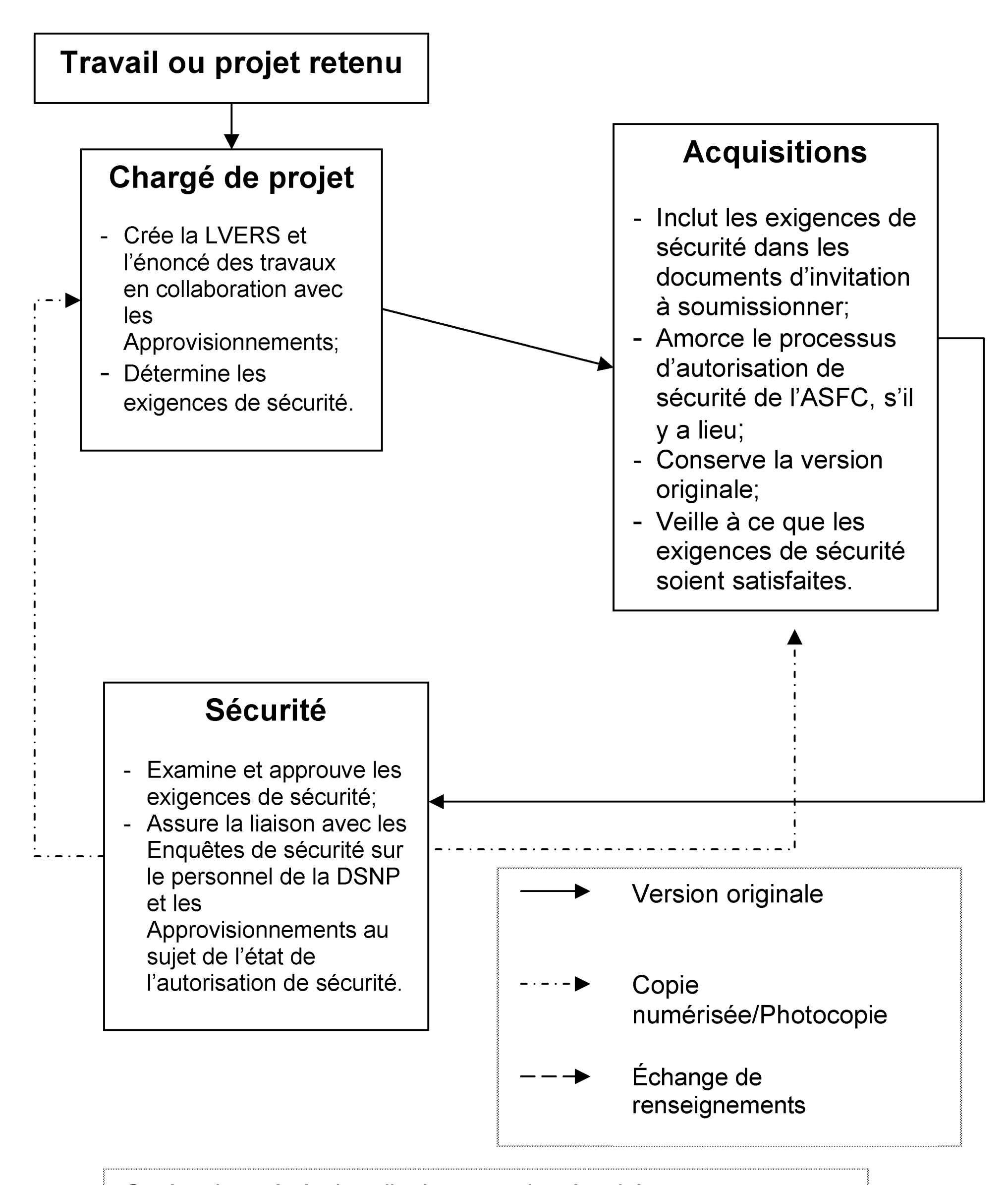
Nota: Jusqu'à nouvel ordre, l'autorisation de sécurité de TPSGC est suffisante pour tous les projets de construction et de location auxquels participe TPSGC.

* Copie papier de la LVERS (l'énoncé des travaux peut être transmis par voie électronique)

**Des catégories générales d'exigences de sécurité sont les suivants:**
- Autorisation de sécurité requise (au niveau établi);
- Accompagnateur seulement;
- Autorisation de sécurité et accompagnateur requis;
- Aucune exigence de sécurité.
- Cote de sécurité d'installation de l'organisation.



*Lorsque TPSGC ne participe pas*




Catégories générales d'exigences de sécurité

- Autorisation de sécurité requise (au niveau établi);
- Accompagnateur seulement;
- Autorisation de sécurité et accompagnateur requis;
- Aucune exigence de sécurité.

**EULEMENT**







## ACTIVITÉS RELATIVES À LA LVERS ET À L'ÉNONCÉ DES TRAVAUX : PARTICIPATION DE L'ASFC SEULEMENT

(Lorsque TPSGC ne participe pas)

Le diagramme ci-dessus démontre les activités relatives à la LVERS et à l'énoncé des travaux lorsque TPSGC ne participe pas:

1. Le travail ou projet est retenu
2. Le chargé de projet crée la LVERS et l'énoncé des travaux en collaboration avec les Approvisionnements et détermine les exigences de sécurité
3. La sécurité examine et approuve les exigences de sécurité, assure la liaison avec les Enquêtes de sécurité sur le personnel de la DSNP et les Approvisionnements au sujet de l'état de l'autorisation de sécurité
4. Les acquisitions inclut les exigences de sécurité dans les documents d'invitation à soumissionner, amorce le processus d'autorisation de sécurité de l'ASFC (s'il y a lieu), conserve la version originale et veille à ce que les exigences de sécurité soient satisfaites.

Nota: Une copie numérisé / photocopie est nécessaire pour le partage d'information.

Nota: Des étapes 2-3 et 3-4, une copie originale est nécessaire. Des étapes 4-1 et 4-3, une copie numérisé / photocopie est nécessaire.

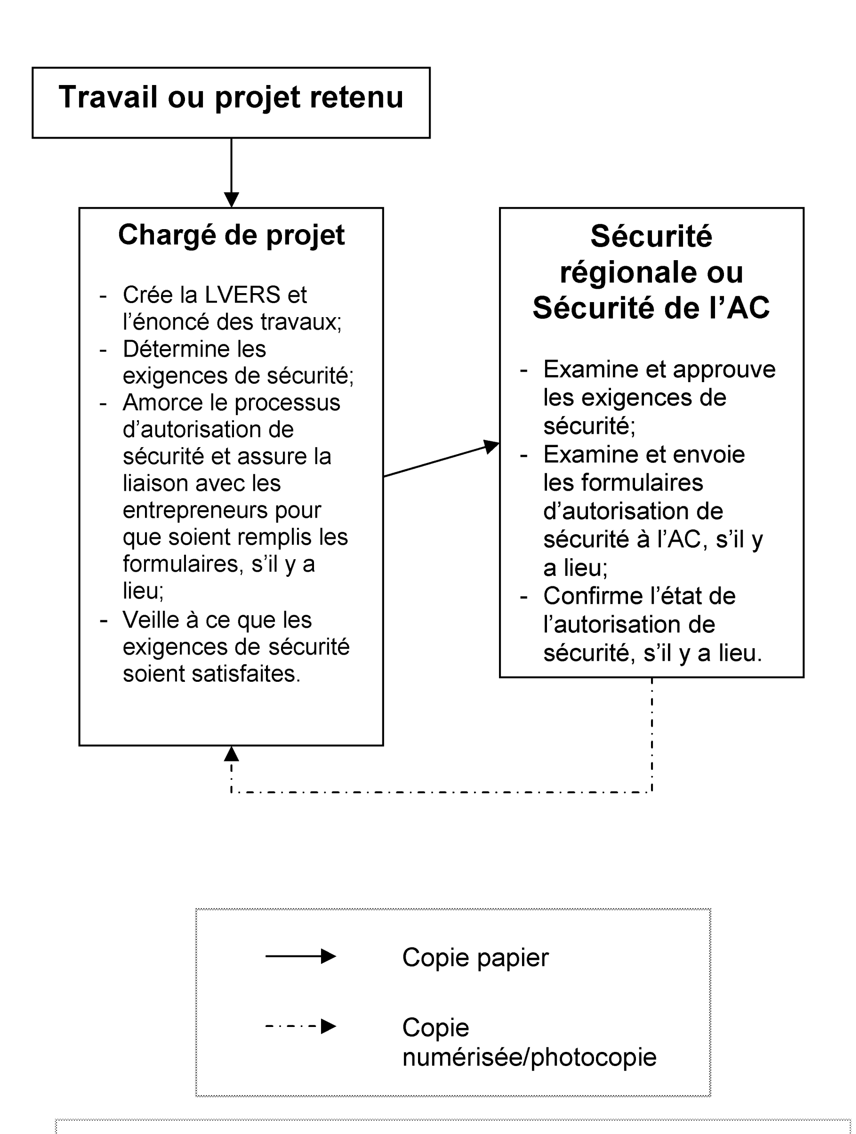
**Des catégories générales d'exigences de sécurité sont les suivants:**

- Autorisation de sécurité requise (au niveau établi);
- Accompagnateur seulement;
- Autorisation de sécurité et accompagnateur requis;
- Aucune exigence de sécurité.





*Lorsque les Approvisionnements de l'ASFC ne participent pas*




Catégories générales d'exigences de sécurité :

- Autorisation de sécurité requise (au niveau établi);
- Accompagnateur seulement;
- Autorisation de sécurité et accompagnateur requis;
- Aucune exigence de sécurité.



**ACTIVITÉS RELATIVES À LA LVERS ET À L'ÉNONCÉ DES TRAVAUX : PARTICIPATION DE L'ASFC SEULEMENT**

(Lorsque les Approvisionnements de l'ASFC ne participent pas)

Le diagramme ci-dessus démontre les activités relatives à la LVERS et à l'énoncé des travaux lorsque l'ASFC ne participe pas:

1. Le travail ou projet est retenu
2. Le chargé de projet crée la LVERS et l'énoncé des travaux, détermine les exigences de sécurité, amorce le processus d'autorisation de sécurité et assure la liaison avec les entrepreneurs pour que soient remplis les formulaires (s'il y a lieu) et veille à ce que les exigences de sécurité soient satisfaites
3. La sécurité régionale ou sécurité de l'AC examine et approuve les exigences de sécurité, examine et envoie les formulaires d'autorisation de sécurité à l'AC (s'il y a lieu) et confirme l'état de l'autorisation de sécurité (s'il y a lieu)

Nota: Des étapes 2-3, une copie originale est nécessaire. Des étapes 3-2, une copie numérisé / photocopie est nécessaire.

**Des catégories générales d'exigences de sécurité sont les suivants:**

- Autorisation de sécurité requise (au niveau établi);
- Accompagnateur seulement;
- Autorisation de sécurité et accompagnateur requis;
- Aucune exigence de sécurité.







## ANNEXE A : FORMULAIRE SUR LES DISPOSITIONS LIÉES À LA SÉCURITÉ

**La présente annexe est réservée en prévision des dispositions normalisées de TPSGC liées à la sécurité des marchés, qui font actuellement l'objet d'un examen par le service des politiques de TPSGC.**







## ANNEXE B : Liste de vérification des exigences relatives à la sécurité

http://publiservice.tbs-sct.gc.ca/tbsf-fsct/350-103-fra.asp







## ANNEXE C : Guide de classification

## GUIDE DE CLASSIFICATION — INFORMATION ET REGISTRES

Épuration des plans :

Il est essentiel que les consultants comprennent l'importance de faire en sorte que les documents et les plans de nature délicate soient manipulés, conservés, transportés, transmis et détruits comme il se doit. Il importe que les consultants comprennent d'abord que les documents sont de nature délicate et qu'ils ne doivent pas être communiqués sans l'autorisation du chargé de projet, et ensuite que le niveau de sensibilité peut nécessiter la mise en place de contrôles précis. Le chargé de projet consultera le service de sécurité afin de déterminer le niveau de sensibilité en jeu.

Il est essentiel de s'assurer que certains renseignements ne figurent pas sur les plans d'exécution avant de les remettre aux entrepreneurs n'ayant pas l'autorisation de sécurité appropriée.

Les plans épurés doivent satisfaire aux critères suivants :

1) Les plans d'exécution ne contiennent aucun plan clé ou plan partiel clé, que ce soit dans la marge ou sur le plan montrant le complexe ou l'emplacement;
2) Les plans d'exécution ne comprennent pas de logos du gouvernement, de nomes ou d'adresses d'emplacements;
3) Les pièces doivent être identifiées par des nombres, et non par des noms. Une liste codée distincte des numéros de pièces associés à des descripteurs et à de l'information de nature délicate doit être établie et mise à jour régulièrement au fur et à mesure que des changements sont faits. Cette liste doit être classée « Protégé B »;
4) L'information sur le système de sécurité et l'information sur les contrôles de sécurité (p. ex. l'information relative au contrôle de l'accès électronique, l'information sur la détection des intrusions) doivent être placées sur des couches distinctes des plans d'exécution afin de rendre plus aisées l'impression et la distribution, et ne doivent pas être remises, même en partie, à des personnes qui n'ont pas obtenu la cote de sécurité adéquate;
5) Les plans conformes à l'exécution ne doivent contenir aucune information que l'on juge de nature délicate comme il est indiqué ci-dessus. Il convient d'indiquer que la conception des pièces est la principale forme de protection des biens délicats, et que la conception des pièces fait aussi partie des mesures de sécurité;
6) Les plans qui ont été épurés doivent porter la mention « Ne pas copier à moins d'avoir obtenu l'autorisation de (inscrire le nom du chargé de projet)/Distribution restreinte ».

### REMARQUES

1) Les types de renseignements suivants générés dans le cadre du projet sont considérés comme délicats :







- Les éléments vulnérables des systèmes, des processus, des procédures ou de l'équipement qui peuvent entraîner des blessures, des blessures graves ou extrêmement graves;
- Toutes les mesures de protection (p. ex. matérielles, du personnel, STI, administratives) qui atténuent les vulnérabilités et/ou les menaces déterminées;
- Les biens/les opérations (p. ex. l'équipement/les opérations de nature délicate/précieuse et l'emplacement qui leur est associé, les armes et leur emplacement, les stupéfiants et leur emplacement, etc.) pour lesquels le fait de savoir peut causer des blessures, des blessures graves ou extrêmement graves;
- Les menaces (p. ex. le vol, le vandalisme, les manifestations, les menaces d'attaque à la bombe, le vol qualifié, etc.) et les opposants qui y sont liés causant des blessures, des blessures graves ou extrêmement graves.

2) Il incombe au rédacteur de déterminer si le document est de nature délicate. Pour ce faire, il doit tenir compte des exigences de sécurité de base communiquées par la Sécurité et s'y conformer.

Remarque : Aux fins du présent projet, le chargé de projet aidera tout consultant qui participe au projet à classifier les documents qu'il crée. Il est essentiel que les consultants étudient le présent document pour comprendre le type d'information qui doit être protégée. En cas de doute, les consultants doivent demander au chargé de projet s'il est important qu'ils ne transportent pas ou ne transmettent pas erronément les documents de nature délicate.

3) Dans certains cas, l'ensemble des documents est de nature délicate, mais certains des documents qui font partie de l'ensemble, pris séparément, sont de nature moins délicate. Ces documents individuels peuvent être communiqués en fonction de leur niveau de sensibilité particulier, mais le chargé de projet ou le distributeur du document doit prendre toutes les mesures raisonnables pour veiller à ce qu'ils ne soient pas distribués de façon à ce qu'on puisse les rassembler.

4) Lors de la transmission des documents de nature délicate, se référer au Guide G1 -009 de la GRC, *Transport et transmission de renseignements protégés ou classifiés*.

Toutes les personnes ayant accès à des biens de nature délicate doivent détenir une autorisation de sécurité valide (accordée à un niveau adapté au niveau de sensibilité en jeu) et elles doivent avoir besoin de cet accès pour pouvoir réaliser les travaux (besoin de connaître). Le chargé de projet est tenu de veiller à ce que toute personne (même celles qui ne sont pas employées) ayant accès à ces biens (y compris les documents) se conforme à ces critères *et* connaisse toutes les mesures de contrôle qu'il faut suivre en tout temps. Le chargé de projet doit aussi veiller à ce que les mesures de sécurité demeurent en vigueur tout au long de la période du marché.

## Conservation des documents de nature délicate

Il faut conserver les documents de nature délicate pour la période établie par le chargé de projet. Il faut manipuler et conserver les documents de nature délicate comme il se doit jusqu'à ce que leur valeur juridique, historique ou archivistique ait expiré. À ce moment, les documents peuvent être détruits au



moyen d'une méthode approuvée. Si l'équipe du projet déclassifie de l'information, on peut en disposer comme des rebuts normaux.

Les documents de nature délicate doivent être retournés à l'Agence lorsqu'elle en fait la demande. Si les documents sont conservés en tant que preuve d'exécution des travaux, l'Agence doit fournir à l'entrepreneur un indicateur adéquat que les travaux ont été effectués si ce dernier prend des mesures en ce sens. Cette situation est traitée au cas par cas.

Quand les documents de nature délicate sont sous le contrôle d'entrepreneurs et de consultants, ils doivent être conservés d'une manière approuvée et seul le personnel qui dispose de l'autorisation de sécurité à jour appropriée peut y accéder. Si l'on soupçonne que des documents de nature délicate ont été compromis, il faut communiquer immédiatement avec le chargé de projet.

## Destruction d'information protégée hors emplacement

Les exigences de sécurité relatives aux services de destruction commerciaux ne visent pas seulement la taille de l'élément. Elles s'appliquent au processus complet de destruction de l'information de nature délicate et elle comprend tout, des procédures de manipulation et de conservation de l'information aux procédures relatives à la disposition des rebuts, en passant par l'installation responsable de la destruction et son personnel.

Il ne faut pas conserver de l'information protégée, même temporairement, dans des installations de destruction commerciales, à moins que l'installation ait une cote de protection des documents délivrée par le PSI de TPSGC.

Si les entreprises de destruction commerciales fournissent des conteneurs pour la collecte et/ou la conservation temporaire de documents protégés en attente de collecte, veuillez communiquer avec le PSI de TPSGC afin de vérifier si le conteneur convient. Il ne faut jamais se servir de conteneurs comportant des fentes pour la conservation temporaire de l'information protégée. Il est possible de se servir de conteneurs comportant des fentes pour la collecte et le transport à l'emplacement de destruction pourvu que ces conteneurs ne servent pas de conteneurs de stockage et qu'ils ne soient pas laissés sans surveillance.

Si vous avez recours aux services d'installations de destruction hors emplacement, veuillez communiquer avec le PSI de TPSGC pour obtenir de l'orientation sur le transport de matériel protégé à cette installation.

Il ne faut pas demander au personnel des installations de destruction commerciales de trier les documents. Afin d'assurer la protection de l'information de nature délicate, les documents doivent être soit triés par du personnel ministériel qui détient la cote de sécurité appropriée avant que ne débute le processus de destruction, soit simplement détruits ensemble selon un processus de destruction doté d'un niveau de sécurité équivalent au niveau le plus élevé attribué aux renseignements de nature délicate. De plus, le tri avant la destruction implique une manipulation du matériel de nature délicate non nécessaire et fait augmenter le risque relatif à la sécurité.







## Services de destruction mobiles

Il faut détruire l'information aussi près que possible du point d'origine, dans une zone isolée et contrôlée. Il est préférable de ne pas procéder à la destruction de l'information de nature délicate dans des allées ou sur des voies publiques.

On donne rarement des autorisations de sécurité aux employés d'entreprises de déchiquetage mobiles en raison de l'instabilité de ces effectifs et des difficultés à tenir à jour les autorisations de sécurité. La destruction de l'information de nature délicate doit être supervisée par un ou des représentants de l'Agence détenant l'autorisation de sécurité appropriée.

## Équipement de destruction approuvé

## Destruction de l'information « Protégé A » et « Protégé B » par déchiquetage, désintégration et broyage

S'applique aux :

Lecteurs de disque dur
Disquettes
CD et DVD
Clés USB
PDA, y compris les BlackBerry et autres dispositifs de mémoire flash (EEPROM)

Les consultants qui souhaitent acheter des déchiqueteuses de bureau approuvées pour la destruction de documents de nature délicate peuvent communiquer avec le PSI de TPSGC afin de se procurer des déchiqueteuses approuvées par l'intermédiaire du bureau du PSI. Le PSI de TPSGC a également une liste d'installations de destruction en grande quantité approuvées si cette méthode de destruction est choisie.

## Destruction de l'information « Protégé A » et « Protégé B » par déchiquetage

S'applique aux : documents papier

Les consultants qui souhaitent acheter des déchiqueteuses de bureau approuvées pour la destruction de documents de nature délicate peuvent communiquer avec le PSI de TPSGC afin de se procurer des déchiqueteuses approuvées par l'intermédiaire du bureau du PSI. Le PSI de TPSGC a également une liste d'installations de destruction en grande quantité approuvées si cette méthode de destruction est choisie.







# LIGNES DIRECTRICES POUR LE SUIVI DE L'INFORMATION DE NATURE DÉLICATE PENDANT LA MANIPULATION, LA DISTRIBUTION ET LA DESTRUCTION

## Généralités

Ce document donne un aperçu des lignes directrices pour effectuer le suivi de l'information de nature délicate pendant la manipulation, la distribution et la destruction et elles doivent être utilisées pendant la conception et la construction des projets de l'Agence. Le but est de repérer le nombre total de plans, de spécifications et de CD.

On s'attend à ce que la majeure partie de l'information, sinon toute l'information de nature délicate associée à ce projet, soit classifiée « Protégé A » ou « Protégé B ». Si vous recevez ou créez d'autres documents dont le niveau de classification est plus élevé, veuillez communiquer avec la Sécurité pour obtenir plus d'orientation.

## Procédures relatives à la manipulation, à la distribution et à la destruction de l'information protégée

Tous les plans et les documents connexes seront créés par le consultant principal. On enverra les originaux au consultant en reproduction pour l'impression du nombre de jeux de documents requis. Lorsque les copies des jeux de documents auront été faites, il faudra les enregistrer avant de les distribuer. Si des jeux de documents supplémentaires sont requis après que la commande originale a été achevée, les jeux de documents supplémentaires seront enregistrés de la même manière, en indiquant le nom des personnes ayant reçu les jeux de documents.

Il faut détruire toutes les copies faites par l'entreprise de reproduction qui ne peuvent servir, qui sont des échantillons pour essai ou simplement le fruit d'erreurs, etc.
La page couverture de chaque jeu de plans sera estampillée avec un bloc de texte.

Sample Block

Drawing Distribution

Set: ______ of ______

Company: ______

Date out: Received SEP 19 2008 MUC Ottawa

Date Returned: ______

VICE • INT

L'image est un bloc d'échantillon « **Sample Block** » avec les informations suivantes :

Drawing Distribution (Distribution du dessin)
Set: *blank* of *blank* (ensemble * de *)
Company: *blank* (compagnie *)
Date out: (date en dehors *)
Date returned: (date de retour *)



Au fur et à mesure que les consultants et les utilisateurs reçoivent les jeux de documents, ils doivent enregistrer chaque jeu reçu en indiquant à qui il a été remis au sein de leur organisation. Chaque document de nature délicate doit faire l'objet de renvois indiquant le moment de réception/de création ainsi que le moment de destruction, et doit être enregistré dans un registre et disponible pour inspection par le chargé de projet. Il faut retourner au chargé de projet tous les documents de nature délicate non détruits à moins qu'ils ne fassent partie des dossiers officiels du consultant. Se référer à la partie sur la conservation des documents de nature délicate. L'information suivante doit être inscrite dans le registre :

a) Numéro de la pièce ou du dossier;

b) Date et heure de réception du document et sa provenance;

c) Nom de la personne qui le reçoit (nom en caractères d'imprimerie et initiales);

d) Titre du document;

e) Description du document (p. ex. : titres des plans et des esquisses);

f) Si l'information a été détruite, nom de la personne avisée et nom de la personne qui a détruit l'information ou qui a supervisé sa destruction;

g) Si l'information a été ramassée, inscrire par quelle personne et à quel moment (heure et date).

Les entrepreneurs ne doivent pas apporter les plans à l'extérieur des lieux des travaux. Ils signent un registre pour les sortir lorsqu'ils en ont besoin et ils les rendent au représentant désigné (inclure le nom du chargé de projet) à la fin de chaque jour de travail. Les entrepreneurs n'ont pas à conserver de copies de plans ou de documents lorsque leur partie du travail est terminée.







La distribution d'information et de plans aux réunions fera l'objet d'une consignation officielle (c.-à-d. numéro, nombre et date). La distribution de ces documents sera notée sur les feuilles de présence et tout document qui n'aura pas été distribué sera immédiatement enregistré comme étant détruit tel qu'il est expliqué dans les présentes lignes directrices. Il incombera au distributeur et au destinataire de faire en sorte que ces documents soient enregistrés dans leur propre système.

Il faut identifier l'information protégée et la traiter comme de l'information de nature délicate jusqu'à ce qu'elle soit déclassifiée ou détruite. Lorsque l'on détruit de l'information protégée, il faut prendre les mesures nécessaires pour assurer la sécurité de l'information pendant sa collecte, sa conservation (même si elle est temporaire), son transport ou sa transmission et sa manipulation pendant la destruction.

Avant la destruction, l'information protégée doit être conservée séparément de l'information déclassifiée ou de l'information non protégée en attente de destruction.

On doit détruire rapidement l'information protégée qui n'a aucune valeur historique ou archivistique et dont la période de conservation a expiré, y compris les copies en surplus, les documents provisoires et les rebuts. Il est nécessaire d'enregistrer la destruction de toute information protégée. Il ne faut pas disposer de l'information protégée par l'intermédiaire d'un programme de recyclage fédéral, provincial, municipal ou privé à moins que l'information protégée n'ait été détruite de manière appropriée approuvée avant le recyclage.

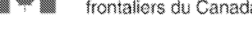
Avant toute destruction de documents, il est nécessaire d'obtenir le consentement écrit du chargé de projet ou de son représentant désigné.

Toute personne qui détruit ou supervise la destruction d'information protégée fait l'objet d'une enquête de sécurité correspondant au niveau de sécurité le plus élevé de l'information à détruire.

Les documents protégés rejetés ou désuets, y compris les plans, sont toujours considérés comme protégés même s'ils ne sont plus pertinents. Il faut les détruire de la manière appropriée et ne pas les considérer comme de l'information non délicate à moins que le personnel de sécurité de l'équipe du projet ne les déclasse et qu'ils deviennent des documents de nature non délicate.








# ANNEXE D : Lignes directrices relatives à la sécurité matérielle et à la TI

## Exigences de sécurité relatives au traitement de l'information protégée dans les systèmes informatiques

L'information non délicate peut être transmise au moyen du réseau de l'organisation et d'Internet.

Il faut traiter l'information protégée sur un ordinateur autonome, dépourvu de toute connexion à un réseau, y compris Internet.

On ne peut autoriser la connexion de l'ordinateur à un système organisationnel, sauf si le PSI de TPSGC a évalué le réseau de l'organisation et déterminé qu'il répond aux exigences du gouvernement du Canada. L'information protégée doit être chiffrée avant d'être portée d'un ordinateur autonome à un ordinateur branché à un réseau à des fins de transmission.

L'information protégée doit être chiffrée en transit et le produit doit être validé en fonction du système de critères communs (http://www.commoncriteriaportal.org/products/) ou selon les directives des responsables de la sécurité de l'ASFC.

Le produit chiffré doit recourir à des algorithmes de chiffrement approuvés par le CSTC pour la protection de l'information protégée (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsa11e-eng_0.pdf ) ou selon les directives des responsables de la sécurité de l'ASFC.

Il est nécessaire de traiter le mot de passe et la phrase passe de chiffrement comme de l'information protégée et de l'échanger de manière sécuritaire, en se servant d'un moyen de communication différent de celui dont on se sert pour le message chiffré (c.-à-d. d'une ligne téléphonique terrestre).

L'information protégée qui n'est plus requise doit être supprimée au moyen d'utilitaires d'effacement sécuritaires qui sont validés en vertu des critères communs, ou le moyen de stockage doit être détruit selon les normes gouvernementales, ou selon les directives des responsables de la sécurité de l'ASFC.

Il faut informer régulièrement les utilisateurs sur la sécurité afin de leur rappeler les pratiques et les politiques en matière de sécurité organisationnelle.

On doit signaler immédiatement à la Sécurité de l'ASFC et au PSI de TPSGC toute infraction ou infraction présumée à la sécurité des systèmes informatiques dont on se sert pour traiter l'information protégée.

L'utilisation d'un ordinateur autonome doté d'une connexion Internet est permise si les conditions suivantes sont respectées :

• Le système d'exploitation informatique doit être conforme à la recommandation en matière de sécurité du document Sommaire – Aperçu des fonctions de sécurité des systèmes d'exploitation/Conseils en



matière de sécurité pour les produits commerciaux (CSPC-1O/S) du CSTC https://www.cse-cst.gc.ca/fr/publication/systemes-dexploitation

• Les mises à jour de sécurité essentielles des applications et du système d'exploitation doivent être vérifiées et exécutées rapidement.

• La protection contre les maliciels est mise en œuvre et les fichiers de données antimaliciels sont mis à jour quotidiennement.

• Un routeur/pare-feu est mis en place entre l'ordinateur et l'Internet et il fournit la traduction d'adresses de réseau (NAT).

• Le navigateur est configuré de manière à empêcher le fonctionnement d'un code mobile non signé (c.-à-d. ActiveX).

• Les programmes utilitaires de contrôle à distance (Remote Desktop Connection, Remote Assistance, PC anywhere) ne sont pas autorisés.

• Un pare-feu logiciel (intégré au système d'exploitation ou ajouté) est mis en service.

• La politique organisationnelle interdit aux utilisateurs de télécharger ou d'utiliser des logiciels non autorisés.

• Un processus de gestion de la configuration et du changement est en place afin d'autoriser localement l'installation de logiciels.

• Les comptes d'utilisateur ne donnent que des privilèges d'accès au système limités.

• L'on sauvegarde l'information protégée sur des supports d'information amovibles qui sont rangés séparément lorsqu'ils ne sont pas utilisés conformément aux exigences relatives à la sécurité matérielle s'appliquant à la classification de l'information protégée (p. ex. l'information classifiée « SECRET » exigera plus de mesures de sécurité matérielle que l'information « PROTÉGÉ B », et moins de mesures de sécurité matérielle seront nécessaires pour l'information « PROTÉGÉ A »).

• L'information classifiée « SECRET » ne doit jamais être visualisée ou conservée sur des systèmes de TI (p. ex. réseau, ordinateur portatif, téléphone, poste de travail autonome, clé USB) qui ne satisfont pas aux exigences de l'ASFC en matière de sécurité matérielle, de sécurité de l'information et de sécurité des TI qui visent les systèmes « SECRET ».

• L'Information « TRÈS SECRET » ne doit jamais être visualisée ou conservée sur des systèmes de TI (p. ex. réseau, ordinateur portatif, téléphone, poste de travail autonome, clé USB); cela est interdit pour des raisons de sécurité.



## EXIGENCES RELATIVES À LA SÉCURITÉ MATÉRIELLE

Il existe un certain nombre de facteurs qui contribuent aux recommandations prévues pour les présentes procédures sur la sécurité dans le cadre du contrat provisoire.

Il faut tenir compte des hypothèses suivantes

- Selon la taille du projet, il peut y avoir ou non des bureaux/des remorques sur place pour la direction de la construction et les sous-traitants. En règle générale, le directeur de la construction/l'entrepreneur général a un bureau ou une remorque pour la plupart des projets.

- La plupart des sous-traitants ont besoin des plans architecturaux, structuraux, mécaniques et électriques complets pour pouvoir coordonner leur travail et remplir des plans d'implantation quotidiens afin que leurs équipes continuent une installation productive. Ces plans et spécifications se trouvent habituellement sur un étage à aire ouverte, sur une table de fortune. N'importe qui peut passer et voir l'information. Ils demeurent généralement dans les zones de travail pendant la nuit, lorsqu'il n'y a personne.

- Si ces articles sont mis sous clé pour la nuit, ils sont habituellement simplement déposés dans un coffre de chantier (ordinairement rien de plus qu'une boîte en contreplaqué munie d'un couvercle et solidement fixée avec une chaîne, qui est fermée à clé ou au moyen d'une combinaison, qui est de style standard et ne comporte pas d'éléments conçus à des fins de sécurité précise).

- Les chantiers de construction sont continuellement fouillés. Il peut arriver dans plusieurs chantiers de construction que des matériaux soient volés et que des coffres de chantier subissent des effractions pour des vols d'outils.

- Très peu de chantiers sont dotés de clôtures externes ou l'on effectue rarement des patrouilles après les heures de travail sur ceux-ci à moins que cela soit prévu au contrat.

Outre les hypothèses ci-dessus, il faut tenir compte des besoins suivants relatifs à la sécurité matérielle. Les besoins se divisent en deux parties : l'environnement de bureau, où sera effectuée la conception, et le chantier de construction, où l'on se sert des plans afin de construire les produits.

## VÉRIFICATION DE SÉCURITÉ DU PERSONNEL

- Les équipes de direction de la construction, d'ingénierie et d'architectes qui travaillent sur le projet doivent avoir les autorisations de sécurité appropriées ou avoir fait l'objet des vérifications nécessaires. Pour ces procédures provisoires, le filtrage de sécurité doit être au moins une







vérification de fiabilité.

• Les représentants de haut niveau des entreprises et les superviseurs sur les lieux doivent se conformer aux mêmes exigences que les architectes, puisqu'ils auront accès à tous les plans et à toutes les spécifications.

• Il ne sera pas nécessaire de vérifier la fiabilité des stagiaires, des ouvriers et des mécaniciens, mais il faudra les superviser en tout temps, et les accompagner aux endroits terminés, occupés ou vulnérables désignés par l'ASFC. Ils ne doivent pas avoir accès aux biens de nature délicate.

BUREAU

Les responsables des immeubles de bureaux et des locaux à bureaux où le personnel contractuel travaillera doivent mettre en place des couches de sécurité similaires à celles qui sont prévues dans les normes de base du gouvernement fédéral (c.-à-d. dans la Politique sur la sécurité du gouvernement) et, s'il y a lieu, à celles des extraits applicables des lignes directrices de la GRC (G1-025). Le PSI de TPSGC fournira des références sur les normes qu'ils doivent satisfaire dans le cadre du Programme de la sécurité industrielle.

1) Il faut sécuriser le périmètre du bureau en question après les heures de travail. On doit munir les portes au minimum d'un verrou et d'un pêne dormant auxiliaire.

2) Il est nécessaire de surveiller électroniquement les locaux à bureaux ou de mettre les plans et les spécifications en sécurité dans une pièce conçue à des fins de sécurité, similaire à ce qui est décrit dans les normes relatives aux pièces sécuritaires de l'ASFC, ou dans un coffre-fort, une caisse ou un classeur similaire à ceux dont on se sert au gouvernement fédéral (muni d'une serrure à combinaison).

3) Le bureau doit permettre la consultation des plans et des spécifications afin que les sous-traitants puissent les examiner aux fins de soumissions.

4) Il faut exercer une surveillance étroite des plans comme l'indiquent les directives fournies dans le cadre du processus d'appel d'offres.

5) Les plans et les spécifications ne font référence aux pièces que par leur numéro. Les noms et la fonction des pièces ne doivent pas être mentionnés à moins que l'utilisateur final détienne une autorisation de sécurité lui permettant de voir de l'information de ce type.

6) Il FAUT s'assurer que certains renseignements ne figurent pas sur les plans et les spécifications des dispositifs de sécurité, des caméras de télévision en circuit fermé et des







enregistreurs numériques lorsque des utilisateurs ne disposant pas de l'autorisation de sécurité devront avoir accès aux plans. Idéalement, la mise en place du câblage pour de tels dispositifs sera prévue dans le contrat de travail de base tandis qu'on lancera un appel d'offres distinct pour la fourniture et l'installation des dispositifs auquel seront invités à soumissionner les entrepreneurs qui ont l'autorisation de sécurité appropriée. Lorsqu'il n'est pas possible de faire des appels d'offres distincts, les détails relatifs à de tels dispositifs et à leurs emplacements doivent être communiqués uniquement au soumissionnaire retenu. Cela repose sur le prix unitaire pour l'offre, et les spécifications ainsi que les schémas d'aménagement sont fournis après l'attribution du marché.

## CHANTIER DE CONSTRUCTION

Il est nécessaire de rassembler les plans et les spécifications chaque jour et de les ranger en lieu sûr dans le bureau de l'entrepreneur général/du directeur de la construction.

- Le bureau de chantier de l'entrepreneur général/du directeur de la construction doit être suffisamment grand pour que l'on puisse y mettre des classeurs sécuritaires dans lesquels tous les sous-traitants mettront leurs plans et leurs spécifications sous clé. Il incombe à l'entrepreneur général/au directeur de la construction d'assurer le contrôle des combinaisons ou des clés de ces classeurs.

- Il reviendra à l'entrepreneur général/au directeur de la construction de s'assurer que tous les plans et toutes les spécifications sont rangés de manière sécuritaire après les heures de travail.

- Le bureau ou la remorque de l'entrepreneur général/du directeur de la construction sera muni d'un système de surveillance comportant des contacts de porte et un détecteur de mouvement déclenchant une alarme pour faire intervenir les services de police ou de sécurité. Il faut aviser l'ASFC de toute alarme de ce type dans les 24 heures.





Canada Border Services Agency | Agence des services frontaliers du Canada



# Directive on Physical Security

This directive takes effect on December 31, 2014.

PROTECTION • SERVICE • INTEGRITY





## Purpose

1. The Directive on Physical Security describes the goals, objectives, core activities and responsibilities of the Physical Security program within CBSA.

## Background

2. Physical Security is based upon the theory that the external and internal design of a facility, and specific security controls, can lead to an environment in which the following is accomplished:
   - The risk of violence towards employees is reduced,
   - The risk of unauthorized access to sensitive assets is reduced, and
   - The risk of disruptions to Agency operations is reduced.

3. This is accomplished by taking certain steps or applying certain measures that are intended to preserve the *confidentiality, integrity, availability and value* of CBSA assets. These steps are referred to as *security controls* and are generally organized in terms of *administrative controls* (such as policies, standards, procedures, etc.), *physical controls* (barriers, lighting, alarms, CCVE, containers, etc.), *procedural controls* (requirements for two-person integrity checks, logging of access) and *technical controls* (design practices). These controls are organized into what are referred to as *protective systems.*

4. These protective systems operate in environments that are in a constant state of change. The Agency's priorities may evolve for a number of reasons, resulting in changes in the prioritization of work and the value of assets. Threats may emerge, evolve or fade with the passage of time. The environment in which the Agency delivers its services may also change depending upon the reach of the agency into the international domain, factors such as climate change, and changes in the demographics of the population. In order to ensure that the protective systems remain relevant to the Agency and continue to function in such a way that the residual Physical Security risk remains within acceptable levels, the protective system evolves within a structure that incorporates the following management practices:
   - The Plan-Do-Check-Act management structure, and
   - Principles of Organizational Resilience*.*

## Objective

5. The objective of this directive is to define the scope of the Physical Security Section activities within the context of the overall set of security controls and policy requirements under the authority of the Deputy Head and Departmental Security Officer (DSO).

## Application







6. This directive applies to all environments, conditions or situations where individuals (regardless of employment status or relationship with the Agency) or entities require access to CBSA personnel, assets or operations.

**Definitions**

7. Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

**Authorities and Sources of Requirements**

8. The authority for decisions made in this directive and within its supporting standards may be derived from many sources including (but not necessarily limited to) the following:
   - International Treaties, Conventions and accepted norms,
   - Legal Requirements (laws, regulations, measures, Orders in Council, and decisions of the Courts),
   - Legal requirements made by provincial, territorial, band or municipal governments where the Privy Council Office (PCO) and Treasury Board of Canada Secretariat (TBS) recognizes the authority of those entities to impose their requirements on the Agency,
   - Government of Canada policies and their supporting standards of identified lead agencies,
   - Public Safety policies where those policies are communicated as requirements placed on CBSA,
   - Overarching CBSA Security policies and authoritative decisions made by the Departmental Security Officer within the context of the authority delegated to that position by the Deputy Head,
   - CBSA policies made by those delegated authority by the Deputy Head, and
   - Decisions that are made in order to maintain the Public Interest and the requirements defined in the Agency's statement of Values and Ethics.
9. Recommendations and decisions made by security practitioners must take into account the individual`s reasonable expectation of receiving a standard of care with respect to safety. This may be described in terms of the "Duty of Care" which includes the following:
   - Identifying those persons or entities that may be impacted, harmed, or put at higher risk directly by a decision,
   - Identifying those persons or entities that may be impacted, harmed or put at higher risk indirectly by a decision, and
   - Being able to demonstrate that reasonable steps have been taken to limit the above.

10. It should be clear that, given the broad range and scope of CBSA activities and infrastructure, the requirements will be defined as applicable to specific cases and that a complete and authoritative list of all authorities will not be maintained.







**Directive Requirements**

11. Physical Security controls are based upon the level and nature of access being proposed. The Physical Security requirements and controls apply to all persons, regardless of their employment status or other relationship with the Agency.

12. Physical Security controls and protective systems must be based on an assessment of risk an accepted risk assessment methodology. Where baseline security controls are being proposed, an assessment of risk must first validate that the baseline security requirements are appropriate for that environment or activity.

    a. Threat and Risk Assessments are intended to be "evergreen" documents. The threat and risk assessment must be reviewed upon any of the following:
        i. An addition of new infrastructure or operations,
        ii. A change in the level of sensitivity in assets or in the criticality of operations,
        iii. A removal of infrastructure or cessation of operations, or
        iv. An overall change in the security controls or detection of a new threat.

13. Those providing security risk management guidance and advice must only provide that guidance or advice within the scope of their administrative responsibilities.
    - Where the physical security risk management guidance pertains to a single region or an activity that is wholly encompassed within a single region, then the guidance falls under the preview of the Regional Security Manager in consultation with the Manager Physical Security and with the Departmental Security Officer having final authority.
    - Where the physical security risk management guidance pertains to multiple regions, is intended to pertain across several regions in the future (such as a pilot project) or pertains to an activity that crosses two or more administrative regions, the guidance shall be provided by the Headquarters in consultation with the regions involved and with the Departmental Security Officer having final authority on the decision.
    - Risk management decisions are constrained and restrained in that they cannot maintain their legitimacy where they put another federal entity (or other partner) at risk or the government as a whole at risk.
14. Physical Security risk management decisions are based upon the information at hand and provided. Consequently, they remain valid for only those periods where such information, its context and its environment have not changed. Where such changes have occurred, the risk assessment must be at least validated as being appropriate.







15. Physical Security risk management guidance and other security guidance shall only be delivered by persons that have the delegated authority to do so.
    a. Those having delegated authority are assumed to have passed a check with respect to possessing an appropriate level of knowledge, skills and experience.

16. Before being given access to any sensitive asset or access to controlled spaces, the individual being proposed to have access must clearly demonstrate the following:
    - The "need to know" or "requirement / right to access" at that particular time and supported by management authorization,
    - A security screening granted at a level commensurate to the level of access being proposed, and
    - The willingness to abide by the physical security requirements associated with the access being proposed.
17. Physical Security controls and protective systems must clearly describe or define the goals or control objectives that they are designed to achieve. Control objectives are to include a measurable and auditable threshold at which point the security control can be declared to be operating effectively.

18. Physical Security controls and protective systems are subject to a range of monitoring and oversight activities. These may include visits, inspections, verifications, stock reconciliations or audits, as appropriate to the specific activity, risks, and past history of the organization. The following restrictions apply in this case:
    - All work must be clearly documented and the outcomes clearly documented,
    - Where an audit or investigation is involved, the party conducting the activity may not audit or investigate its own work,
    - A follow up plan must be included and agreed upon as part of the submission, and
    - Any instance where self-assessments are used, any claims must be supported by documentation.
19. The monitoring and oversight activities constitute activities that are endorsed by senior management. A failure to participate, provide complete or provide accurate information is considered to be a security violation and may also fall within the scope of the Agency's integrity monitoring activities (Professional Standards Investigation).

20. Failure to abide by the physical security requirements may result in administrative, civil or criminal proceedings, as assessed on a case-by-case basis and taking into account the specific circumstances that apply.

**Security Incidents**



21. All personnel must report any security incident, security violation or security breach upon discovery and in accordance with the standards put forward by the Security Incident Reporting Coordinator. It must also remain clear that all suspected breaches of law must be reported to the appropriate law enforcement body.

    a. Failure to report incidents, or delaying doing so, may result in the continued exposure of such information to compromise, aggravate an already undesirable security situation, hamper investigative action and delay the determination and application of corrective measures.

**Standards**

22. Physical Security will produce standards associated with program-level activities that describe the mandatory and suggested practices to be adhered to within the scope of those programs. These standards are considered to be authoritative with respect to the specific requirements of those programs.

23. The specific direction given in security standards must have its basis on any one or more of the following:
    - Legislated or regulatory requirements,
    - Agreements with international, national, provincial or other partners,
    - Government of Canada policies, including the direction given by lead agencies,
    - Departmental policies and practices, or
    - Security doctrine as practiced by a recognized professional association.
24. Where security equipment or technology is proposed, such technology must meet any one or more of the following criteria as determined by the Physical Security section:
    - Accreditation by a lead agency of the federal government with responsibilities in the Physical Security domain.
    - Accreditation by an impartial, scientific laboratory which has been accredited or accepted by an international body or industry associated with the management and mitigation of security risk in that particular domain, or
    - Accreditation through scientific testing where such tests comply with the norms or standards used to determine the nature, limit and suitability of materials or installations as mitigating measures.
25. Where standards or similar mechanisms are produced with respect to the protection of persons, assets, or the continuity of operations, they must be done in consultation with the Physical Security Section.

**Procedures**







26. Procedures issued as recommendations by the Physical Security program are considered to be security controls and carry the same weight as recommendations associated with other forms of security controls.

**Accountabilities and Responsibilities**

27. The *Departmental Security Officer (DSO),* as the delegate of the Deputy Head, has the final authority on security risk management decisions within the Agency.

28. The *Director Infrastructure and Information Security* oversees the Physical Security section's activity, ensuring its alignment with Agency priorities and other elements of the Agency's security program.

29. In addition to the formulation of Physical Security policy, the *Physical Security section* will produce other guidance material, tools and aids in support of program-level activities. This guidance is considered to be authoritative in its own right, dependent upon the source of the requirements being adhered to.

30. The *Manager Physical Security* acts as the senior functional authority for Physical Security within the Agency, providing authoritative guidance and advice on technical matters of Physical Security.

31. *The Security Policy* section may provide guidance based on the approved documentation submitted by the Physical Security section. In any case where such guidance is given, the Manager Physical Security must be informed and may overturn the guidance if appropriate.

32. *Regional Security Managers* provide subject matter expertise within the context of the Physical Security program within their administrative areas. Regional Security Managers also assist by providing environmental and situational awareness to the program from within their administrative areas.

33. *Security Advisors within the Physical Security section* provide subject matter expertise and program support on a range of topics. Security advisors speak authoritatively on the security requirements associated with their program support activities and assigned areas of responsibility.

34. *Regional Security Officers* provide support to the Regional Security Manager in meeting the requirements and obligations within the Physical Security program. Regional Security Officers also assist in this effort by providing environmental and situational awareness to the program through the Regional Security Manager.

35. The *Security in Contracting Management Coordinator* provides subject matter expertise and authoritative guidance on matters involving the requirements for Security Requirement Checklists, the development of the Physical Security element of Security Guides, the inspection of private







sector facilities and the requirement to ensure appropriate oversight and monitoring of security requirements where work is being performed by private sector entities.

36. The *Controlled Assets Coordinator* provides subject matter expertise and authoritative guidance within the Security Controlled Assets program on matters such as the issuance, distribution, handling, storage, maintenance, control and removal of service of the controlled assets that fall within the scope of the program.

37. The *Security Incident Reporting Coordinator* acts as the central coordination point for the reporting of Security incidents and provides authoritative guidance on matters such as the requirements to report in addition to the communication, content, distribution, and use of the reports and information falling within the scope of the security reporting activity.

38. The *Physical Security Training Coordinator* acts as the central coordination point for the technical content of all security training for those that are assigned Physical Security functions or responsibilities within the Agency.

**Enquiries**

39. Enquiries should be directed to the Manager, Physical Security.





Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive sur la sécurité matérielle

PROTECTION • SERVICE • INTÉGRITÉ

Canada



Cette directive entre en vigueur le 31 décembre 2014.

**But**

1. La directive sur la sécurité matérielle décrit les buts, les objectifs, les activités principales et les responsabilités liés au programme de sécurité matérielle au sein de l'Agence des services frontaliers du Canada (ASFC).

**Contexte**

2. La sécurité matérielle est fondée sur la théorie selon laquelle la conception externe et interne d'une installation et des contrôles de sécurité particuliers peuvent entraîner un environnement où les objectifs suivants sont atteints :
   - Le risque de violence à l'égard des employés est réduit;
   - Le risque d'accès non autorisé à des biens de nature délicate est réduit;
   - Le risque de perturbation des activités de l'Agence est réduit.

3. À cette fin, on prend ou on applique certaines mesures qui visent à préserver *la confidentialité*, l'*intégrité*, la *disponibilité* et la *valeur* des biens de l'ASFC. Ces mesures sont des *contrôles de sécurité* et sont généralement organisées sous forme de *contrôles administratifs* (notamment des politiques, des normes, des procédures, etc.), de *contrôles physiques* (barrières, éclairage, avertisseurs, matériel vidéo en circuit fermé [MVCF], contenants, etc.), de *contrôles procéduraux* (exigences en matière de contrôles d'intégrité par deux personnes et d'enregistrement de l'accès) et de *contrôles techniques* (pratiques de conception). Ces contrôles sont regroupés dans des *systèmes de protection.*

4. Les systèmes de protection fonctionnent dans des environnements qui évoluent continuellement. Les priorités de l'Agence peuvent évoluer pour un certain nombre de raisons, ce qui peut modifier l'ordre de priorité des tâches et la valeur des biens. Des menaces peuvent se présenter, évoluer ou s'estomper au fil du temps. L'environnement dans lequel l'Agence assure ses services peut aussi évoluer selon la portée de cette dernière dans le domaine international, des facteurs tels que le changement climatique et des changements sur le plan des caractéristiques démographiques de la population. Afin de veiller à ce que les systèmes de protection demeurent pertinents pour l'Agence et qu'ils continuent de fonctionner de sorte que le risque résiduel pour la sécurité matérielle demeure à un niveau acceptable, le système de protection évolue à l'intérieur d'une structure qui comporte les pratiques de gestion suivantes :
   - Structure de gestion planifier, faire, vérifier, agir;
   - Principes de résilience organisationnelle.

**Objectif**







5. La directive vise à définir la portée des activités de la Section de la sécurité matérielle dans le contexte de l'ensemble des contrôles de sécurité et des exigences de la politique qui relèvent de l'autorité de l'administrateur général et de l'agent de la sécurité du ministère (ASM).

**Application**

6. Cette directive s'applique à l'ensemble des environnements, des conditions ou des situations dans lesquels des personnes (indépendamment de leur statut d'emploi ou de leur relation avec l'Agence) ou des entités doivent avoir accès au personnel, aux biens ou aux opérations de l'ASFC.

**Définitions**

7. Des définitions précises provenant de sources qui font autorité se trouvent au Glossaire des termes de sécurité.

**Autorités et sources d'exigences**

8. L'autorité concernant les décisions prises en vertu de la présente directive et des normes à l'appui peut découler de nombreuses sources, notamment (mais non de façon limitative) les sources suivantes :
   - Traités internationaux, conventions et normes reconnues;
   - Exigences juridiques (lois, règlements, mesures, décrets et décisions des tribunaux);
   - Exigences juridiques établies par les gouvernements provinciaux ou territoriaux, les administrations de bandes ou les administrations municipales, lorsque le Bureau du Conseil privé (BCP) et le Secrétariat du Conseil du Trésor du Canada (SCT) reconnaissent le pouvoir de ces entités d'imposer leurs exigences à l'Agence;
   - Politiques du gouvernement du Canada et normes à l'appui des organismes responsables;
   - Politiques relatives à la sécurité publique, lorsque celles-ci sont communiquées à titre d'exigences imposées à l'ASFC;
   - Politiques générales de l'ASFC en matière de sécurité et décisions faisant autorité prises par l'ASM en vertu des pouvoirs délégués à ce poste par l'administrateur général;
   - Politiques de l'ASFC élaborées en vertu des pouvoirs délégués par l'administrateur général;
   - Décisions prises afin de maintenir l'intérêt public et les exigences définies dans l'énoncé des valeurs et de l'éthique de l'Agence.
9. Les recommandations et les décisions des spécialistes de la sécurité doivent tenir compte du fait que la personne s'attend raisonnablement à obtenir une norme de diligence en matière de sécurité. Il peut s'agir d'une « obligation de diligence », qui englobe ce qui suit :
   - Identifier les personnes ou les entités qui peuvent être touchées directement par une décision, ou subir des dommages ou être exposées à un risque accru à la suite de celle-ci;
   - Identifier les personnes ou les entités qui peuvent être touchées indirectement par une décision, ou subir des dommages ou être exposées à un risque accru à la suite de celle-ci;







- Pouvoir démontrer que des mesures raisonnables ont été prises afin de limiter les conséquences ci-dessus.

10. Il doit être clair que compte tenu de la gamme et de la portée étendues des activités et des infrastructures de l'ASFC, les exigences seront définies selon des cas particuliers, et qu'on ne tiendra pas de liste exhaustive et faisant autorité des pouvoirs.

**Exigences de la directive**

11. Les contrôles de sécurité matérielle sont fondés sur le niveau et la nature de l'accès proposé. Les exigences en matière de sécurité matérielle s'appliquent à toutes les personnes, indépendamment de leur statut d'emploi ou de leurs relations avec l'Agence.

12. Les contrôles de sécurité matérielle et les systèmes de protection doivent être fondés sur une évaluation des risques selon une méthode reconnue d'évaluation des risques. Lorsque des contrôles de sécurité de base sont proposés, une évaluation des risques doit d'abord confirmer que les exigences de base en matière de sécurité conviennent à l'environnement ou à l'activité.

    a. Les évaluations de la menace et des risques sont censées constituer des documents « évolutifs ». L'évaluation de la menace et des risques doit être révisée dans les situations suivantes :
        i. Ajout d'une nouvelle infrastructure ou de nouvelles opérations;
        ii. Changement de niveau de sensibilité de biens ou de la criticité d'opérations;
        iii. Enlèvement d'une infrastructure ou arrêt d'opérations;
        iv. Changement global de contrôles de sécurité ou détection d'une nouvelle menace.

13. Les personnes qui offrent des conseils et des avis en matière de gestion des risques pour la sécurité doivent offrir ces conseils et ces avis dans le cadre de leurs responsabilités administratives.
    - Lorsque des conseils relatifs à la gestion des risques pour la sécurité matérielle concernent une région particulière ou une activité menée entièrement dans une région, les conseils sont du ressort du gestionnaire régional de la sécurité, en collaboration avec le gestionnaire de la sécurité matérielle et l'ASM, à titre d'autorité de dernière instance.
    - Lorsque des conseils relatifs à la gestion des risques pour la sécurité matérielle touchent plusieurs régions, qu'ils doivent toucher ultérieurement plusieurs régions (comme dans le cas d'un projet pilote) ou qu'ils touchent une activité qui recoupe au moins deux régions administratives, les conseils doivent être fournis par l'administration centrale, en collaboration avec les régions concernées et avec l'ASM, à titre d'autorité de dernière instance.
    - Les décisions de gestion des risques sont soumises à des contraintes et à des restrictions en ce sens qu'elles ne peuvent pas demeurer légitimes lorsqu'elles entraînent un risque pour une autre entité fédérale (ou un autre partenaire fédéral) ou pour l'ensemble du gouvernement.



14. Les décisions concernant la gestion des risques pour la sécurité matérielle sont fondées sur l'information disponible et sur celle qui est fournie. Ainsi, elles demeurent valides uniquement pendant la période où l'information, son contexte et son environnement ne changent pas. Lorsque ces éléments changent, on doit au moins valider la pertinence de l'évaluation des risques.
15. Seules les personnes qui disposent du pouvoir délégué pertinent peuvent fournir des conseils liés à la gestion des risques pour la sécurité matérielle et d'autres conseils en matière de sécurité.
    a. On présume que les personnes dotées d'un pouvoir délégué ont fait l'objet d'une vérification visant à déterminer si elles possèdent un niveau approprié de connaissances, de compétences et d'expérience.

16. Avant d'avoir accès à un bien de nature délicate ou à un espace contrôlé, une personne doit montrer clairement qu'elle respecte les critères suivants :
    - Le « besoin de connaître » ou le « besoin ou droit d'accès » à ce moment particulier, appuyé par l'autorisation de la direction;
    - Une enquête de sécurité approuvée à un niveau qui correspond au niveau d'accès proposé;
    - La volonté de respecter les exigences en matière de sécurité matérielle liées à l'accès proposé.
17. Les contrôles de sécurité matérielle et les systèmes de protection doivent décrire ou définir clairement les buts ou les objectifs de contrôle qu'ils sont censés atteindre. Les objectifs de contrôle doivent comporter un seuil mesurable et auditable auquel on peut déclarer que le contrôle de sécurité fonctionne efficacement.

18. Les contrôles de sécurité matérielle et les systèmes de protection font l'objet de diverses activités de contrôle et de surveillance, par exemple des visites, des inspections, des mécanismes de concordance des stocks ou des auditions, selon l'activité, les risques et les antécédents de l'organisation. Les restrictions suivantes s'appliquent dans ce contexte :
    - Les tâches et les résultats doivent être clairement consignés;
    - En cas d'audit ou d'enquête, la partie qui mène l'activité ne peut pas effectuer un audit ou une enquête visant son propre travail;
    - Un plan de suivi doit être inclus et convenu dans la présentation;
    - Toute conclusion provenant d'une autoévaluation doit être documentée.

19. Les activités de contrôle et de surveillance sont approuvées par la haute direction. Le défaut de participer ou de fournir des renseignements complets ou exacts est considéré comme une atteinte à la sécurité, et peut également relever des activités de surveillance de l'intégrité de l'Agence (enquête relative aux normes professionnelles).

20. Le défaut de respecter les exigences en matière de sécurité matérielle peut entraîner des poursuites administratives, civiles ou criminelles, déterminées au cas par cas selon les circonstances particulières applicables.

**Incidents de sécurité**







21. Tous les employés doivent signaler les incidents de sécurité, les atteintes à la sécurité ou les infractions à la sécurité lorsqu'ils les découvrent, et conformément aux normes établies par le coordonnateur des rapports d'incidents de sécurité. En outre, il doit être clair que les infractions présumées à la loi doivent être signalées à l'organe compétent d'exécution de la loi.

    a. Si on omet de signaler un incident, ou si on tarde à le faire, cela risque de mettre encore en péril des renseignements de nature délicate, d'aggraver une situation déjà préjudiciable à la sécurité, d'entraver une enquête et de retarder l'application de mesures correctives.

**Normes**

22. La Section de la sécurité matérielle élabore des normes liées aux activités de programmes qui décrivent les pratiques obligatoires et proposées qui doivent être respectées dans le cadre des programmes. Ces normes sont considérées comme faisant autorité en ce qui a trait aux exigences précises des programmes.

23. L'orientation énoncée dans les normes de sécurité doit être fondée sur un ou plusieurs des éléments suivants :
    - Exigences législatives ou réglementaires;
    - Accords avec des partenaires internationaux, nationaux, provinciaux ou d'autres partenaires;
    - Politiques du gouvernement du Canada, y compris les orientations fournies par les organismes responsables;
    - Politiques et pratiques ministérielles;
    - Doctrine de sécurité appliquée par une association professionnelle reconnue.

24. Lorsque du matériel ou des technologies de sécurité sont proposés, ils doivent respecter un ou plusieurs des critères suivants déterminés par la Section de la sécurité matérielle :
    - Accréditation par un organisme responsable du gouvernement fédéral qui assume des responsabilités dans le domaine de la sécurité matérielle.
    - Accréditation par un laboratoire scientifique impartial agréé ou reconnu par un organisme international ou une industrie associée à la gestion et à l'atténuation des risques pour la sécurité dans ce domaine particulier;
    - Accréditation fondée sur des essais scientifiques conformes aux normes utilisées pour déterminer la nature, les limites et la pertinence de matériel ou d'installations en guise de mesures d'atténuation.

25. Lorsque des normes ou des mécanismes semblables sont produits en ce qui concerne la protection des personnes ou des biens ou la continuité des opérations, ils doivent être élaborés en collaboration avec la Section de la sécurité matérielle.







**Procédures**

26. Les procédures diffusées en tant que recommandations découlant du programme de sécurité matérielle sont considérées comme des contrôles de sécurité, et ont le même poids que les recommandations liées à d'autres formes de contrôles de sécurité.

**Reddition de comptes et responsabilités**

27. En tant que représentant délégué de l'administrateur général, l'ASM dispose de l'autorité de dernière instance en ce qui concerne les décisions touchant la gestion des risques pour la sécurité au sein de l'Agence.

28. Le *directeur, Division de l'infrastructure et de la sécurité de l'information* supervise les activités de la Section de la sécurité matérielle, en s'assurant qu'elles correspondent aux priorités de l'Agence et aux autres éléments du programme de sécurité de cette dernière.

29. Outre la formulation de la Directive sur la sécurité matérielle, la *Section de la sécurité matérielle* produit des documents d'orientation, des outils et des aides à l'appui des activités de programme. On considère que ces éléments d'orientation font autorité en soi, selon la source des exigences à respecter.

30. Le *gestionnaire de la sécurité matérielle* agit à titre d'autorité fonctionnelle supérieure en matière de sécurité matérielle au sein de l'Agence, et fournit une orientation et des conseils qui font autorité sur des questions techniques liées à la sécurité matérielle.

31. La section de la *politique relative à la sécurité* peut offrir des conseils fondés sur la documentation approuvée soumise par la Section de la sécurité matérielle. Lorsque des conseils sont ainsi fournis, le gestionnaire de la sécurité matérielle doit être informé, et peut invalider les conseils le cas échéant.

32. Les *gestionnaires régionaux de la sécurité* offrent une expertise en la matière dans le contexte du programme de sécurité matérielle dans leurs régions administratives. Ils peuvent également contribuer une connaissance de l'environnement et de la situation au programme du point de vue de leur région administrative.

33. Les *conseillers en sécurité de la Section de la sécurité matérielle* offrent une expertise en la matière et un appui aux programmes relativement à divers sujets. Les conseillers en sécurité parlent avec







autorité au sujet des exigences liées à leurs activités en matière d'appui aux programmes et à leur secteur de responsabilité.

34. *Les agents régionaux de sécurité* aident le gestionnaire régional de la sécurité à satisfaire aux exigences et aux obligations du programme de sécurité matérielle. Les agents régionaux de sécurité collaborent également à ces efforts en fournissant une connaissance de l'environnement et de la situation au programme par l'intermédiaire du gestionnaire régional de la sécurité.

35. Le *coordonnateur de la gestion des marchés* en matière de sécurité offre une expertise en la matière et des conseils faisant autorité sur les questions touchant les exigences relatives à la Liste de vérification des exigences relatives à la sécurité, l'élaboration des éléments relatifs à la sécurité matérielle dans les guides de sécurité, l'inspection des installations du secteur privé et l'obligation d'assurer une surveillance et un contrôle appropriés des exigences de sécurité lorsque le travail est effectué par des entités du secteur privé.

36. Le *coordonnateur des biens contrôlés* offre une expertise en la matière et des conseils faisant autorité dans le cadre du programme des biens contrôlés de sécurité relativement à des questions telles que la délivrance, la distribution, la manutention, l'entreposage, l'entretien, le contrôle et l'enlèvement de services liés aux biens contrôlés qui relèvent du programme.

37. Le *coordonnateur des rapports d'incidents de sécurité* assure la coordination centrale des rapports d'incidents de sécurité et offre des conseils faisant autorité sur des questions telles que l'obligation de signaler les incidents, outre la communication, le contenu, la distribution et l'utilisation des rapports et l'information visée par les activités de rapports de sécurité.

38. Le *coordonnateur de la formation en matière de sécurité matérielle* assure la coordination centrale du contenu technique de la formation liée à la sécurité pour les personnes qui assument des fonctions et des responsabilités relatives à la sécurité matérielle au sein de l'Agence.

**Demandes de renseignements**

39. Les demandes de renseignements doivent être transmises au gestionnaire de la sécurité matérielle.





Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for Physical Security Risk Management

PROTECTION • SERVICE • INTEGRITY





This standard takes effect on December 31, 2014.

**Purpose**

1. This standard provides guidance with respect to the management of Physical Security risk. This standard includes requirements (indicated by *must, shall, or will*) and recommendations (indicated by *should, might, or may*).

**Intent**

2. The intent of this document is to provide clear, concise guidance with respect to the various requirements of the Physical Security Risk Management process to those involved in the following:
    a. Physical Security Threat Analyses,
    b. Physical Security Threat Assessments,
    c. Physical Security Vulnerability Analyses,
    d. Physical Security Vulnerability Assessments,
    e. Physical Security Risk Analyses, and
    f. Physical Security Risk Assessments.
3. The Physical Security Risk Management processes are used when determining the specific Physical Security goals, Physical Security control objectives, and specific Physical Security controls.

**Scope**

4. This standard pertains to all activities where an individual is required to provide guidance, advice or direct services (such as the conduct of Threat and Risk Assessments) with respect to the establishment of Physical Security controls or other similar measures intended to protect the Physical Security of persons, sensitive assets or the continuity of operations.

**Requirements**

*General*

5. All Physical Security controls must be based upon an assessment of risk. Where a baseline measure is being proposed, an assessment of risk must have been conducted and validated in terms of supporting the use of baseline standards.
6. Only approved tools and methodologies shall be used for the conduct of Threat and Risk Assessment or Physical Security risk assessments.
7. All those performing Physical Security Threat and Risk Assessments must be appropriately delegated to conduct those activities.







8. Before two or more methodologies are used to assess risk, they must be related to each other so that the various values and outputs can be directly related to each other with minimal probability of misinterpretation. This is often referred to as undergoing a check for interoperability.

Methodologies and Specific Guidance

*Prioritization*

9. The prioritization of sites based on Physical Security risks shall be coordinated through the Physical Security Section (PSS) of the Security and Professional Standards Directorate (SPSD) and the Departmental Security Officer (DSO).
10. The PSS of SPSD shall produce the working tools to be used by the regions and other stakeholders in this respect. These tools shall take into account the communicated priorities of the Agency.

*Conduct of Vulnerability Assessments*

11. Vulnerability assessments are used to identify personnel, infrastructure, or operations that may be, by their nature, more susceptible to targeting by attackers. The PSS of SPSD shall provide tools that allow for this assessment to be undertaken.
12. The methodology to be used in this respect is a combination of the CARVER+S and MSHARPP methodologies.
    a. CARVER refers to a methodology that has the assessor use all information within an organization to identify particularly vulnerable infrastructure points.
    b. MSHARPP refers to a methodology that has the assessor use information and resources that may be reasonably available to the attacker and, taking into account the past history of the attacker, uses that information to identify particularly vulnerable infrastructure points.

*Conduct of Threat and Risk Assessments*

13. The conduct of Physical Security Threat and Risk Assessments (TRA) shall use the Royal Canadian Mounted Police (RCMP) / Communications Security Establishment Canada (CSEC) Harmonized Threat and Risk Assessment (HTRA) methodology.
    a. ***Risk*** in the HTRA methodology is a factor of asset value, threat, and vulnerability.
    b. ***Asset value*** shall be determined using guidance provided by the Treasury Board of Canada and lead agency documentation and shall take into account the following at a minimum:
        i. Confidentiality in terms of the potential impacts associated with unauthorized disclosure,
        ii. Integrity in terms of the potential impacts associated with the unauthorized addition, modification, or deletion of assets (as appropriate) or its handling through untrusted processes,







iii. Availability in terms of the ability to call upon and use the good or service as intended,
iv. Dollar value in terms of financial limits established for purposes of assessing the financial impacts of events and communicated in the HTRA, and
v. Social or cultural value in terms of the potential loss or damage to assets that have particular cultural or social significance.

c. Threat values are based upon a combination of gravity and likelihood, as defined in the HTRA methodology and as included in tools provided by Physical Security. The following considerations apply:
   i. When considering gravity, the definitions in the HTRA methodology are to be used. Where such definitions are not clearly defined, the Physical Security tools shall be used to provide guidance.
   ii. When considering likelihood, the scalar used for the HTRA shall be used to determine the score associated with both past and future events. For example, if an event is expected to happen every ten days or is assessed as being likely to happen every ten days, then the result that would be associated with the event happening ten days ago will be used.
d. Vulnerability values shall be conducted based upon the definition provided in the HTRA guidance material. This includes the following:
   i. Preventive controls shall be assessed based upon their ability to deter, delay or deny the progress of the attacker.
   ii. Detection, response and recovery controls shall be based upon the following:
      1. the ability to identify suspicious or suspect behaviour,
      2. the ability to categorize such behaviour,
      3. the ability to notify the appropriate point of contact for the response,
      4. the ability to trigger an appropriate response with a reasonable expectation of containing and halting the attack and
      5. The ability to put in place conditions for the recovery to optimal levels of operations.
   iii. Vulnerabilities may also be determined based upon the available means and opportunity available to the attacker in a specific situation. This must then be related to the above.
e. The scalars used for identifying the level of risk are defined within the HTRA methodology and are arrived at by multiplying the scores associated with the Asset Value, Threat, and Vulnerability (as defined in the HTRA guidance material).
f. The level of risk shall be linked in terms of the following three elements:
   i. The specific score (such as a score of 18 of 125),
   ii. The label associated with the specific score (very low to very high), and
   iii. The guidance associated with the recommendation towards management's position towards the level of identified risk (definitely acceptable to definitely unacceptable).







*Recommendations based on Physical Security Risk Assessment*

14. Recommendations made in response to risks identified in the Threat and Risk Assessment shall fall into one of the following categories of response:
    a. ***Mitigating*** the risk by reducing the impacts or likelihood associated with the identified risk
    b. ***Transferring*** the risk by having another organization assume responsibility for taking steps to mitigate the risk as per the above. It must be noted that transferring the risk to another organization does not absolve the organization from its accountabilities associated with the risk,
    c. ***Sharing*** the risk by mitigating one part of the risk while transferring aspects of the risk to a third party,
    d. ***Avoiding*** the risk by changing operations, environment or infrastructure in such a way that the risk, if assessed after the change, would not be present, and
    e. ***Accepting*** the risk where appropriate to do so and in line with an individual's delegated authority within the Agency. It should be noted that the senior officer able to accept Physical Security risk is the Departmental Security Officer (DSO) as the delegate of the Deputy.
15. Recommendations must clearly describe how they would lead to a lower residual risk. They do this primarily through the reduction of vulnerabilities but may also include steps that affect the value of the asset or threat. In all cases, the physical security control must incorporate the following elements:
    a. A description of the physical security control (control) and the physical security risk criteria,
    b. The means of measuring the performance of the control and its relationship to the risk criteria, and
    c. The means of collecting the measurements and monitoring the effectiveness of the security control.
    d. Those designing security controls (safeguards) must remain aware that the inappropriate design of such controls may leave assets exposed to risk, operations vulnerable to disruption or other undesirable conditions.
16. Recommendations made with respect to the management of risk must take into account the following:
    a. Legal and regulatory requirements,
    b. The direction provided by Government of Canada lead agencies,
    c. Agreements made with partners and stakeholders, and
    d. Previous decisions of senior management, including directions as to how to respond to similar circumstances.
17. The following guidance shall be used to link management decisions with the recommendations coming from the assessment of risk:
    a. Where management is required (or has communicated its authoritative intent) to prevent the injuries associated with the risk, preventive controls are to be put in place that can be reasonably expected to deter or stop the attack,







b. Where management is required to manage (indicated through terms such as minimize, etc.) risk, then security goals and criteria must be clearly identified and linked to the security controls being proposed, and
c. Where management has accepted risk, security criteria and controls must be established to monitor conditions so as to detect and notify senior management of changes in the residual risk that was accepted.

*Provision of Guidance*

18. Recommendations regarding protective systems and security controls are based on an assessment of risk.
19. In making risk management recommendations, the primary focus shall be on the management of vulnerabilities. This is because the general values associated with assets and threats will be relatively constant.
20. In this context, the mathematical steps based upon the HTRA methodology and described in Appendix A are taken to arrive at the controls that will be used to reduce the vulnerabilities being addressed.

*Documentation of Results and Protection of Documentation*

21. All Prioritization Exercises, Vulnerability Assessments, and Threat and Risk Assessments must be documented and include the basis upon which values are arrived at.
22. All information, in all forms, contained in such documentation (or other media) must be protected in accordance with its level of sensitivity.
23. All information contained in such documentation must also be assessed in terms of its ability to be exempted under the *Access to Information Act*, particularly in terms of any information pertaining to threats and vulnerabilities.
24. All documentation must be strictly controlled based on the principle of the need to know. Only those persons that are directly involved in the design, occupation, management or oversight of the subject of the Threat and Risk Assessment *within the Agency* can demonstrate a legitimate need to know without first validating the need to know with the PSS of SPSD.

*Reviews and Renewals*

25. Physical Security Threat and Risk Assessments are intended to be managed in such a way as to remain continuously relevant.
26. The review of the Threat and Risk Assessment shall be based on a risk-based approach. The review shall be undertaken so that the Threat and Risk Assessment is reviewed not less than once every five





years. It should be clear that this review may be undertaken more frequently based on the following:

a. The ***criticality*** (in the context of national critical infrastructure) of the facility or services delivered at the services that warrant a greater degree of oversight or where there is less tolerance for allowing a vulnerability to persist. Examples of this may include, but are not necessarily limited to, key transportation nodes, key service delivery points, locations where critical assets are maintained, etc. This may result in an increase in the rate or in the nature of the oversight activities,
b. ***Agreements*** that require that oversight activities meet specific thresholds in order to maintain the agreement in force (such as an Agreement that specifies that a certain facility must be inspected annually),
c. ***Agency senior management risk management decisions*** regarding the level of confidence that must be maintained with respect to the protection of personnel, assets (including information) and the continuity of operations.

27. In addition to the review cycle identified above, Threat and Risk Assessment will likely be reviewed when the following conditions are identified:
    a. Upon a change in operations,
    b. Upon a change in infrastructure, or
    c. Upon a change in security goals or security control criteria (such as through a change in management decisions regarding the level of acceptable residual risk).

**Roles and Responsibilities**

28. The Security Executive Management Committee provides direction with respect to the intent of the Agency to manage its overall security posture.
29. The Departmental Security Officer (DSO) acts as the senior officer and sole authority to accept security risk, including residual risk, as the delegate of the Deputy Head.
30. The Director Infrastructure and Information Security provides oversight of the Physical Security Threat and Assessment activity, ensuring that it aligns with the overall direction of the Agency.
31. The Manager, Physical Security acts as the senior functional authority with respect to the conduct of Physical Security risk and vulnerability assessment activities.

**Supporting Material**

32. This standard falls under the Directive on Physical Security.
33. This standard operates in conjunction with the following additional standards:
    a. Standard for Physical Security Design
    b. Standard for Access Control
    c. Standard for Controlled Assets
    d. Standard for Physical Security Monitoring and Oversight

**Enquiries**





34. Enquiries are to be forwarded to the Manager, Physical Security.



**Appendix A – Structure for Guidance**

35. The following structure is to be used when providing Physical Security guidance. This structure closely follows that of the HTRA methodology:
    a. Identify the scope of the question and ensure it is clearly defined.
    b. Identify the assets to be protected.
    c. Identify any specific threats that are apparent in the environment
    d. Identify any existing security controls and how they are arranged into a protective system
    e. Identify the core vulnerabilities
    f. Identify the range at which management intends to manage the risk
    g. Identify the lowest and highest values assigned to that range of risk
    h. Run the calculation V=R/(AxT) for each of the upper and lower risk value
    i. The resulting score for vulnerability is the score that would be derived from the vulnerability score,
    j. Rounding the score down will yield the vulnerability score that would need to be achieved to be clearly within the limits established by management. The next whole number above this number would be the closest option associated with managing risk.
36. The resulting numbers are compared to the outcomes that would be arrived at if using the tables for preventive controls and detection, response, and recovery controls.
37. Consider the following example:
    a. Management wishes to protect persons from a threat involving potential loss of life when they are working outside the facility.
        i. The asset being protected is an individual at risk of physical harm up to loss of life. This equates to a HIGH value when following the HTRA guidance (A=4)
    b. Consider that the threat assessment identifies the threat as being moderate in nature when taking into account both gravity and likelihood (V=3)
    c. This yield a value of twelve when multiplying the asset value and the threat.
        i. V=R/(A x T) where A=4 and T=3
    d. Consider the circumstance in which management wishes to manage at a moderate level of risk, but no higher.
        i. The low range / score for this would be 15 and the higher score would be 32.
        ii. The vulnerability score at the low range would be 15/12 or 1.25. This means that the vulnerability score that would be acceptable is one.
        iii. For the higher score, the calculation would be 32 /12 or 2.66.
        iv. As a result, a vulnerability score of either one or two would be considered acceptable.
        v. These scores would align with a VERY LOW or LOW vulnerability score.
    e. Those designing the security controls would then design the preventive controls and detection / response / recovery so that protective system aligned with the VERY LOW or LOW categories.





Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme sur la gestion du risque en matière de la sécurité matérielle

PROTECTION • SERVICE • INTÉGRITÉ





Cette norme entre en vigueur le 31 décembre 2014.

**Objet**

1. La présente norme propose des directives concernant la gestion du risque en matière de sécurité matérielle. Elle comprend des exigences (indiquées par les verbes *doit (doivent) ou devra (devront)*) et des recommandations (indiquées par les verbes *devrait (devraient) ou peut (peuvent)*).

**Intention**

2. L'intention du présent document est de fournir des directives claires et précises sur diverses exigences du processus de gestion du risque en matière de sécurité matérielle pour ceux et celles qui prennent part aux activités suivantes :
   a. Analyse de la menace en matière de sécurité matérielle;
   b. Évaluation de la menace en matière de sécurité matérielle;
   c. Analyse de la vulnérabilité en matière de sécurité matérielle;
   d. Évaluation de la vulnérabilité en matière de sécurité matérielle;
   e. Analyse du risque en matière de sécurité matérielle;
   f. Évaluation du risque en matière de sécurité matérielle.
3. On a recours aux processus de gestion du risque en matière de sécurité matérielle pour déterminer les buts particuliers de la sécurité matérielle, les objectifs des contrôles de sécurité matérielle et les contrôles de sécurité matérielle particuliers.

**Champ d'application**

4. La présente norme vise toutes les activités dans le cadre desquelles on demande à une personne de fournir de l'orientation, des conseils ou d'offrir directement une prestation de services (comme la réalisation d'évaluations en matière de menace et de risque) concernant l'établissement de contrôles de sécurité matérielle ou d'autres mesures du genre visant à assurer la sécurité matérielle des personnes, des biens sensibles ou la continuité des opérations.

**Exigences**

*Stipulations générales*

5. Tous les contrôles de sécurité matérielle doivent se fonder sur une évaluation du risque. Quand une exigence de base en matière de sécurité est proposée, il faut préalablement qu'une évaluation du risque ait été réalisée et validée afin de justifier l'utilisation de cette exigence de base.







6. seulement les outils et les méthodologies ayant fait l'objet d'une approbation pour la réalisation de l'évaluation de la menace et des risques ou les évaluations des risques en matière de sécurité matérielle.
7. Toutes les personnes procédant aux évaluations de la menace et des risques en matière de sécurité matérielle doivent avoir été déléguées comme il convient pour pouvoir exercer ces activités.
8. Avant d'avoir recours à deux méthodologies ou plus pour l'évaluation du risque, il faut s'assurer qu'elles sont liées entre elles, afin que le lien entre les différentes valeurs et données de sortie soit direct et que la probabilité d'une mauvaise interprétation soit réduite au minimum. C'est ce qu'on appelle communément effectuer une vérification d'interopérabilité.

Méthodologies et directives particulières

*Priorisation*

9. La priorisation de sites fondée sur le risque en matière de sécurité matérielle devra être coordonnée par l'intermédiaire de la Section de la sécurité matérielle de la Direction de la sécurité et des normes professionnelles (DSNP) et de l'agent de sécurité du ministère (ASM).
10. La Section de la sécurité matérielle de la DSNP devra fournir les outils de travail que les régions et les autres intervenants utiliseront à cet égard. Ces outils devront tenir compte des priorités ayant déjà été communiquées par l'Agence.

*Réalisation de l'évaluation de la vulnérabilité*

11. On se sert de l'évaluation de la vulnérabilité pour repérer les membres du personnel, les parties de l'infrastructure ou les opérations qui, de par leur nature, sont plus susceptibles d'être la cible de ceux qui commettent des attaques. La Section de la sécurité matérielle de la DSNP devra fournir les outils permettant de réaliser cette évaluation.
12. À cet égard, il convient de se servir d'une combinaison des méthodes CARVER+X et MSHARPP.
    a. La méthode CARVER fait référence à une méthode selon laquelle l'évaluateur utilise toute l'information à sa disposition au sein d'un organisme pour repérer les points particulièrement vulnérables dans l'infrastructure.
    b. La méthode MSHARPP fait référence à une méthodologie selon laquelle l'évaluateur utilise l'information et les ressources pouvant raisonnablement être mises à la disposition de la personne qui commet des attaques, tout en tenant compte de ses antécédents, et se sert de cette information pour repérer les points particulièrement vulnérables dans l'infrastructure.

*Réalisation de l'évaluation de la menace et des risques*

13. L'évaluation de la menace et des risques (EMR) en matière de sécurité matérielle doit être réalisée selon la méthodologie harmonisée d'évaluation de la menace et des risques (EMR) de la







Gendarmerie Royale du Canada (GRC) /du Centre de la sécurité des télécommunications Canada (CSTC).

a. Le ***risque***, dans la méthodologie harmonisée EMR, est un facteur de valeur des biens, de menace et de vulnérabilité.
b. La ***valeur des biens*** doit être déterminée sur la base des directives fournies par le Conseil du Trésor du Canada et figurant dans la documentation de l'organisme responsable, et doit, au moins, tenir compte de ce qui suit :
    i. La confidentialité, en fonction des répercussions potentielles associées à la divulgation non autorisée;
    ii. L'intégrité, en fonction des répercussions potentielles associées à l'ajout, à la modification ou à la suppression de biens non autorisés (le cas échéant) ou à leur traitement par l'intermédiaire de processus non éprouvés;
    iii. La disponibilité, en fonction de la capacité d'utiliser des biens et des services et d'y avoir recours, comme prévu;
    iv. La valeur du dollar, en fonction des limites financières ayant été établies aux fins d'évaluation des répercussions financières des événements et qui ont été communiquées dans la méthodologie harmonisée EMR;
    v. La valeur sociale ou culturelle, en fonction de la perte ou des dommages potentiels pouvant toucher des biens ayant une importance culturelle ou sociale particulière.
c. Les valeurs de la menace sont fondées sur une combinaison de la gravité et de la probabilité, selon les définitions de la méthodologie harmonisée EMR et les indications des outils fournis par la sécurité matérielle. Les considérations suivantes s'appliquent :
    i. Lorsque l'on considère la question de la gravité, il faut se servir des définitions de la méthodologie harmonisée EMR. Quand ces définitions manquent de précision, il faut se référer aux outils en matière de sécurité matérielle, qui fournissent de l'orientation.
    ii. Lorsque l'on considère la question de la probabilité, il faut se servir du scalaire de la méthodologie harmonisée EMR pour déterminer la cote associée aux événements passés et futurs. Par exemple, s'il est prévu qu'un événement se produise tous les dix jours ou, selon l'évaluation, cet événement est susceptible de se produire tous les dix jours, on utilisera alors le résultat qu'on associerait à l'événement survenu il y a dix jours.
d. Le calcul des valeurs de la vulnérabilité doit être fait en se fondant sur la définition figurant dans les documents d'orientation de la méthodologie harmonisée EMR. Ce calcul comprend ce qui suit :
    i. L'évaluation des contrôles de prévention, fondée sur leur capacité à prévenir, à retarder ou à effacer le progrès de celui qui commet des attaques.
    ii. Les contrôles de la détection, de la réponse et de la récupération, qui doit se fonder sur ce qui suit :



1. la capacité de repérer un comportement louche ou suspect;
2. la capacité de catégoriser un tel comportement;
3. la capacité de signaler le point de contact adéquat pour la réponse;
4. la capacité d'apporter une réponse adéquate permettant d'être raisonnablement en droit de s'attendre à ce qu'on puisse maîtriser et freiner l'attaque;
5. La capacité de mettre en place des conditions permettant la récupération des niveaux optimaux des opérations.

iii. Il est également possible de déterminer la vulnérabilité en se fondant sur les moyens disponibles et les possibilités s'offrant à celui qui commet des attaques dans une situation précise. Ce calcul doit par la suite être mis en rapport avec ce qui précède.

e. Pour établir la valeur des scalaires utilisés pour déterminer le niveau de risque, qui sont définis conformément à la méthodologie harmonisée EMR, il faut multiplier les cotes associées à la valeur des biens, de la menace et de la vulnérabilité (conformément à la définition figurant dans les documents d'orientation de la méthodologie harmonisée EMR).

f. Le niveau de risque doit être lié en fonction des trois éléments suivants :
   i. La cote précise (comme une cote de 18 sur 125);
   ii. L'étiquette associée à la cote précise (très faible à très élevé);
   iii. Les directives associées à la recommandation à l'égard de la position de la direction en ce qui touche le niveau de risque constaté (parfaitement acceptable à parfaitement inacceptable).

*Recommandations fondées sur l'évaluation du risque en matière de sécurité matérielle*

14. Les recommandations formulées comme suite aux risques définis dans l'évaluation de la menace et du risque doivent être classées dans une des catégories de réponses suivantes :
   a. L'***atténuation*** du risque, en réduisant les répercussions ou la probabilité associée aux risques ayant été définis;
   b. Le ***transfert*** du risque, en faisant assumer par un autre organisme la responsabilité de prendre les mesures nécessaires pour atténuer le risque, comme indiqué plus haut. Rappelons que le transfert du risque à un autre organisme ne dispense pas l'organisme de ses responsabilités associées au risque;
   c. Le ***partage*** du risque, en atténuant une partie du risque tout en en transférant certains aspects à une tierce partie;
   d. L'***évitement*** du risque, en modifiant les opérations, l'environnement ou l'infrastructure de façon à ce que le risque, s'il est évalué après la modification, ne soit plus présent;
   e. L'***acceptation*** du risque, lorsque cela s'avère opportun et conforme à une personne disposant de pouvoirs délégués au sein de l'Agence. Soulignons que l'agent supérieur en







mesure d'accepter le risque en matière de sécurité matérielle est l'agent de sécurité du Ministère (ASM) à titre de délégué du sous-ministre.

15. Les recommandations doivent clairement décrire de quelle façon elles se traduiraient par un risque résiduel de niveau moindre. On y arrive principalement par la réduction de la vulnérabilité, mais il est également possible d'y inclure des étapes ayant une incidence sur la valeur du bien ou de la menace. Dans tous les cas, le contrôle de la sécurité matérielle doit intégrer les éléments suivants :
    a. Une description du contrôle de la sécurité matérielle (contrôle) et des critères de risque en matière de sécurité matérielle;
    b. Les moyens de mesurer l'efficacité du contrôle et ses relations aux critères en matière de risque;
    c. Les moyens de recueillir les mesures et de suivre de près l'efficacité du contrôle de la sécurité.
    d. Les personnes qui assurent la conception des contrôles de sécurité (dispositifs de protection) ne doivent pas perdre de vue qu'une conception inadéquate de tels contrôles peut exposer les biens à des risques, rendre les opérations vulnérables aux interruptions ou se traduire par d'autres conditions non souhaitées.
16. La formulation de recommandations en lien avec la gestion du risque doit tenir compte de ce qui suit :
    a. Les exigences juridiques et réglementaires;
    b. Les directives fournies par les agences responsables du gouvernement du Canada;
    c. Les ententes conclues avec les partenaires et les intervenants;
    d. Les décisions antérieures de la haute direction, notamment les directives concernant la façon de réagir en pareilles circonstances.
17. Les directives suivantes doivent être respectées lors de l'établissement d'un lien entre les décisions de la direction et les recommandations émanant de la gestion du risque :
    a. Lorsque la direction est tenue (ou a fait part de son intention autoritaire) de prévenir les blessures associées au risque, des contrôles de prévention dont on est raisonnablement en droit de s'attendre à ce qu'ils préviennent ou stoppent l'attaque doivent être mis en place;
    b. Lorsque la direction est tenue d'assurer la gestion du risque (indiqué par des expressions comme réduire au minimum, etc.), les objectifs et les critères en matière de sécurité doivent alors être clairement définis et mis en relation avec les contrôles proposés en matière de sécurité;
    c. Une fois que la direction a accepté de gérer le risque, des critères et des contrôles en matière de sécurité doivent être établis afin de suivre de près les conditions et d'être en mesure de détecter et de signaler à la haute direction les modifications apportées au risque résiduel ayant été acceptées.

*Prestation de directives*



18. Les recommandations concernant les systèmes de protection et les contrôles de sécurité sont fondées sur une évaluation du risque.
19. Lors de la formulation de recommandations en matière de gestion du risque, l'objectif principal doit être la gestion de la vulnérabilité. Ceci est dû au fait que les valeurs générales associées aux biens et aux menaces seront relativement constantes.
20. Dans ce contexte, on se sert d'étapes mathématiques fondées sur la méthodologie harmonisée EMR et décrites à l'Annexe A pour en arriver aux valeurs du contrôle qui seront utilisées pour réduire les vulnérabilités en cause.

*Documentation des résultats et protection de la documentation*

21. Tous les exercices d'établissement des priorités, les évaluations de la vulnérabilité et les évaluations de la menace et du risque doivent être documentés, et doivent y figurer les fondements ayant servi à établir les valeurs.
22. Toute l'information, sous toutes ses formes, contenue dans des documents du genre (ou dans d'autres moyens de communication), doit être protégée conformément à son degré de sensibilité.
23. Toute l'information contenue dans des documents du genre doit également faire l'objet d'une évaluation, en ce qui concerne sa capacité à bénéficier d'une exemption en vertu de la *Loi sur l'accès à l'information*, plus particulièrement en ce qui a trait à toute information relative à la menace et à la vulnérabilité.
24. Toute la documentation doit être strictement contrôlée sur la base du principe du besoin de connaître. Seules les personnes participant directement à la conception, à l'occupation, à la gestion ou à la surveillance de l'objet de l'évaluation de la menace et des risques *au sein de l'Agence* ont le droit de démontrer le besoin légitime de connaître sans avoir d'abord à le faire valider auprès de la Section de la sécurité matérielle de la DSPN.

*Examens et renouvellements*

25. Les évaluations du risque et de la menace pour la sécurité matérielle sont conçues pour demeurer d'actualité.
26. L'examen de l'évaluation du risque et de la menace devrait se fonder sur une approche axée sur les risques et devrait être effectué au moins une fois tous les cinq ans. Il faut bien comprendre que la fréquence de cet examen peut être plus élevée dans les circonstances décrites ci-dessous.
    a. La ***criticité*** (dans le contexte d'une infrastructure nationale essentielle) de l'installation ou des services justifie une surveillance accrue ou la tolérance envers une vulnérabilité constante est moindre. Voici une liste non exhaustive d'exemples : nœuds de transports importants, points de prestation de services importants, lieu de conservation de biens essentiels, etc. Ceci peut entraîner une augmentation de la fréquence ou de la portée des activités de surveillance.



b. ***L'entente*** exige que les activités de surveillance respectent certains seuils pour qu'elle demeure en vigueur (comme une entente précisant qu'une certaine installation doit être inspectée chaque année).

c. ***Les décisions de la haute direction de l'Agence sur la gestion des risques*** concernent le niveau de confiance qu'il faut conserver en ce qui a trait à la protection du personnel, à la protection des biens (y compris l'information) et à la continuité des opérations.

27. En plus des examens prévus dans le cycle décrit précédemment, l'évaluation de la menace et des risques est susceptible de faire l'objet d'un examen dans les conditions suivantes :
    a. les opérations font l'objet d'un changement;
    b. l'infrastructure fait l'objet d'un changement;
    c. les objectifs en matière de sécurité ou les critères relatifs aux contrôles de sécurité font l'objet d'un changement (comme un changement dans les décisions de la direction sur le niveau de risque résiduel acceptable).

**Rôles et responsabilités**

28. Le Comité exécutif responsable de la sécurité fournit des directives sur l'intention de l'Agence de gérer sa position générale en matière de sécurité.
29. L'agent de sécurité du ministère (ASM) agit à titre de cadre supérieur et il est le seul à pouvoir accepter le risque pour la sécurité, y compris le risque résiduel, à titre de délégué de l'administrateur général.
30. Le directeur responsable de la sécurité de l'information et de l'infrastructure assure la surveillance des activités d'évaluation et des activités relatives à la menace pour la sécurité matérielle et veille à ce que ces activités s'harmonisent avec l'orientation générale de l'Agence.
31. Le gestionnaire responsable de la sécurité matérielle agit à titre d'autorité fonctionnelle principale en ce qui a trait à la réalisation des activités d'évaluation de la vulnérabilité et du risque pour la sécurité matérielle.

**Documents pertinents**

32. La présente norme est régie par la Directive sur la sécurité matérielle.
33. La norme s'applique conjointement avec les normes suivantes :
    a. Norme de conception de la sécurité matérielle;
    b. Norme pour le contrôle d'accès;
    c. Norme visant les biens contrôlés;
    d. Norme sur le contrôle et la surveillance de la sécurité matérielle.

**Demandes**

34. Les demandes doivent être acheminées au gestionnaire responsable de la sécurité matérielle.



**Annexe A – Étapes à suivre pour formuler des directives**

35. Les étapes énumérées ci-dessous s'appliquent lorsqu'une personne formule des directives sur la sécurité matérielle. Ces étapes suivent de près celles de la méthodologie harmonisée EMR :
    a. établir la portée de la question et veiller à ce qu'elle soit bien définie;
    b. déterminer les biens qui doivent être protégés;
    c. relever toute menace précise qui est apparente dans le milieu;
    d. déterminer les contrôles de sécurité en place et la façon dont ils sont organisés pour créer un système de protection;
    e. déterminer les vulnérabilités fondamentales;
    f. déterminer dans quelle mesure la direction a l'intention de gérer le risque;
    g. établir les seuils inférieur et supérieur attribués à cette gamme de risques;
    h. effectuer le calcul Vulnérabilité=Risque/(Bien x Menace) pour tous les seuils de risque inférieurs et supérieurs;
    i. la cote ainsi obtenue pour la vulnérabilité est celle qui serait obtenue à partir de la cote relative à la vulnérabilité;
    j. l'arrondissement par défaut de la cote donnera la cote relative à la vulnérabilité qu'il faut atteindre pour respecter clairement les limites établies par la direction. Le nombre entier immédiatement supérieur à ce nombre est l'option la plus rapprochée en ce qui concerne la gestion du risque.
36. Les nombres ainsi obtenus sont comparés aux résultats qui seraient obtenus si on avait utilisé les tableaux destinés à évaluer les contrôles de prévention, la détection, la réaction et les contrôles de reprise.
37. Prenons l'exemple ci-dessous.
    a. La direction souhaite protéger des personnes contre une menace pouvant mettre leur vie en danger lorsqu'elles travaillent à l'extérieur des installations.
        i. Le bien protégé est une personne qui est exposée à des dommages physiques et à la perte de vie. Ceci correspond à une valeur ÉLEVÉE en application de la méthodologie harmonisée EMR (B=4).
    b. Supposons que l'évaluation de la menace révèle que la menace est moyenne compte tenu de la gravité et de la probabilité (V=3).
    c. Le produit de la valeur du bien et de la menace est 12.
        i. V=R/(B x M), où B=4 et M=3.
    d. Supposons que la direction souhaite gérer un risque moyen, tout au plus.
        i. La cote/gamme la plus faible de ce risque serait 15 et la cote la plus élevée serait 32.
        ii. La cote relative à la vulnérabilité pour la gamme la plus faible serait 15/12, soit 1,25. Ainsi, la cote de sécurité acceptable se chiffrerait à 1.
        iii. Pour la cote la plus élevée, le calcul serait de 32/12, soit 2,66.







iv. Par conséquent, si la cote de sécurité se chiffre à 1 ou à 2, elle serait considérée comme acceptable.

v. Ces cotes correspondraient à une cote relative à la vulnérabilité TRÈS FAIBLE ou FAIBLE.

e. Les personnes responsables de la conception des contrôles de sécurité concevraient alors les contrôles de prévention, la détection, la réaction et la reprise afin que le système de protection corresponde aux catégories TRÈS FAIBLE ou FAIBLE.






# Standard for Physical Security Design

PROTECTION • SERVICE • INTEGRITY





This standard takes effect on December 31, 2014.

Purpose

1. The purpose of this document is to provide a functional security design based on approved Physical Security Risk Management (see standard). This standard includes requirements and recommendations.

Intent

2. The intent of this document is to provide clear, concise direction with respect to the various requirements incorporated into all CBSA (Agency) physical security designs. It provides a CBSA goal based security design with the flexibility to address specific needs while maintaining an overall national standard for physical security design. It will provide a foundation for baseline design that may be applied to personnel, infrastructure, information or operations.
3. This document is intended to provide direction that will ensure the Agency's adherence to the four main physical security considerations. These are as follows:
   a. Layers of defence,
   b. Clearly discernible zones,
   c. The concept of protection, detection, response and recovery, and
   d. The integration of enhanced security in response to foreseeable (up to an including imminent) heightened or elevated threat environments.
4. This standard is intended to work alongside other CBSA physical security standards
   a. As a foundation for the Standard for Physical Security *Monitoring and Oversight* through the integration of measurement criteria into the specific design of controls, and
   b. As a response to the Standard for *Physical Security Risk Management* as describing the process to be used when designing physical security controls used to address risk management issues
5. This standard is intended to assist in the management of Physical Security risk through the following:
   a. Designing to control exceptional threats in the public spaces;
   b. Designing the perimeter of the facility so as to allow for a reasonably consistent level of residual risk within the facility,
   c. Maintaining appropriate access control, layers of defence, protective systems (based on protection, detection, response, and recovery), taking into account any potential increase in threat level, and
   d. Designing specific infrastructure points (such as rooms) based on the risks associated with the protection of personnel, assets and operations.







Scope

6. This standard pertains to all activities with respect to the establishment of physical security controls and other similar measures intended to protect the physical security of persons, assets (including information) and the ability to maintain an environment conducive to operations.

7. This standard applies to all infrastructure throughout all points of the lifecycle. It includes new builds, renovations and retrofits, regardless of location, or whether the property is owned, loaned or leased.

8. Physical Security design must begin with an assessment of risk. Dependent on the level of risk and likelihood of the threat being manifested, security controls will be recommended such that they interact to mitigate all physical risk to acceptable levels.

Security Application

*Any assessment of risk must be conducted by an appropriately delegated subject matter expert in their specific field of expertise.*

The Departmental Security Officer (DSO) and the Security Organization bear the responsibility of ensuring the safeguarding of personnel, information, sensitive operations, and the facilities in which we conduct business. The simplest and most reasonable means of meeting all of these obligations is achieved through the layered application of physical security controls to a facility.

9. The first step in this process is ensuring that the appropriate zoning requirements are identified. The definitions and requirements for public, reception, operations, security and high security zones are drawn directly from the *Operational Standard for Physical Security (Section 6.2 – Hierarchy of Zones)*. The step immediately following this is to ensure that there are an appropriate number of layers of defense around those zones.

10. When designing layers of defence, the outcome of the security design must result in at least the following:

   a. Protection immediately around the asset (such as a secure container);
   b. At least two layers of protection between the layer protecting the asset directly and the perimeter marking the edge of the span of control, (such as a fence marking the edge of property). These layers may not be subject to the same vulnerability nor may they use the same token or means of passing through the barrier (such as both barriers using the same access badge or credential);







c. Each internal barrier will incorporate the principles associated with protection, detection, response and recovery described below; and

d. The final layer being the perimeter control that divides the space where the Agency exercises a span of *control* from those spaces where it can only *influence* controls (such as the edge of the property).

11. The concept of protection, detection, response and recovery – refers to controls being used to delay an attacker to the point where there is a reasonable expectation that an effective response can arrive and halt the progress of the attack before the attacker is successful. This may involve reaching an asset or even simply eroding trust by being able to remain present unchallenged in controlled areas. This is described more fully below in the section focussing on *layers of defence*.

12. An appropriate security posture is realized by incorporating layers of defence and the principles above, those layers being determined by the following:

a. The value of the asset being protected,

b. The environment in which the controls are operating, and

c. The level of assurance that must be maintained that the overall security controls will be effective in preventing the attack.

13. In general, security controls may be communicated through the following:

a. Through the results of a specific Threat and Risk Assessment conducted under the authority of the DSO,

b. Through a standard that is developed for common infrastructure and which only apply in those cases where the assets, operations, and identified risks are similar to being at the point where they are indistinguishable when compared, and

c. Through the direction of the DSO in any media or form where the DSO is exercising his risk management authority over security risk.

14. To be considered appropriate, security controls must meet or exceed the following criteria:

a. They must be based upon an assessment of risk and have a reasonable expectation of meeting the security goals and objectives identified in managing that security risk, and

b. The control must be able to demonstrate that it meets the requirements of credible security design authorities. Credible security design authorities may include recognized experts referring to sound and accepted practices, accredited associations, accredited laboratories or certified testing centers. The latter of these are often found in industry associations such as the Underwriters Laboratories (UL), etc.







c. The control must ensure that it meets or exceeds the requirements of applicable laws, regulations and codes.

d. It should be noted that the Policy on Government Security and other lead agency standards are minimum standards and it should be understood that where CBSA faces an increased level of apparent risk, it may choose to operate above these baseline standards. Baseline standards should not be used as the basis for design until an assessment of risk has been conducted and Physical Security has validated that the risk environment is appropriate to those baselines.

15. Security controls must also be measurable. This will also include identifying the threshold at which the standard can be described as functioning as intended.

a. The measurement requirement is an important and integral part of the monitoring and oversight process and must be integrated into the design,

b. The measurement requirement must also be able to be related back to the reducing of risk back to acceptable (to management) levels, and

c. The description of the measurement and records of the measurement must meet the auditing criteria of being attestable, repeatable, and appropriately documented.

16. Security controls must also be maintained throughout their lifecycle. It is important, at the designing phase, to ensure that this is clearly identified and takes into account operational, environmental and other changes.

Roles and Responsibilities

17. Design experts must incorporate security design into their project plans and specifications. Tendering agents for CBSA (including PWGSC) must be aware of, and must adhere to the security restrictions found within the Communication and Coordination Protocol: Between CBSA Infrastructure. They must ensure that all companies submitting a tender meet the required Designated Organization Screening (DOS) or the Private Sector Organizational Screening with Information/Document handling.

18. Failing to incorporate security within the design process can lead to the unnecessary damage or disruption of personnel, infrastructure or even expensive retrofits.

19. The Office of Principal Interest (OPI) and their tendering authority must ensure Security Requirement Checklists, Statement of Requirements, Statement of Work, Statement of Sensitivity and all other pre-tender documentation is properly completed and provided to the appropriate local Security Office (IT and Physical) for incorporation of the security requirements for the contract and







for the construction of the facility. All Regional recommendations are subject to DSO sign off through the Security and Professional Standards Directorate – Physical Corporate Security

20. CBSA Operations Branch is the OPI for site construction. CBSA Operations Branch is responsible for providing their operational requirements. This includes proper completion of their Statement of Requirements (identifying work spaces needed and to some extent the preferred location of that space). Other critical documentation to be completed includes,

- Statement of Sensitivity – This identifies areas of higher security requirements based on the needs of each function within the facility. For example, they may justify the need for a Secure Discussion Area, or for high security zones for classified operations.
- Security Requirement Checklist and the Statement of Work will be completed jointly with Infrastructure or the Construction Management team.

21. Regional Security offices are responsible for conducting an assessment of the property on which the structures are to be built. They review drawings and specifications and provide security requirements based on the Risk Assessment of the property. If risk levels are sufficiently low, they may adapt this baseline application to the project. If risk levels are such that risk is elevated, then appropriate enhanced security elements will be recommended. All resolutions must be reviewed and signed off by or for the DSO.

22. Security and Professional Standards Directorate (SPSD) is responsible for the development of all security direction documents such as Standard, Procedures, Guidelines, Directives and Bulletins. They review or conduct Threat and Risk Assessments on the physical security of each facility. They review all construction plans and specifications, ensuring the appropriate security elements are in place and properly protected as per the Security and Infrastructure Protocol. They monitor on-going construction directly or indirectly through Infrastructure and Regional Security reporting. They inspect completed facilities to ensure all security elements are present and functioning properly, and to verify those elements do address and mitigate the risk as expected. Finally, they ensure the site is regularly reviewed; confirming the security profile still meets the security needs.

Enquiries

23. Enquiries are to be forwarded to the Manager, Physical Security via the Physical Security mailbox.

CBSA-ASFC_DSO_Physical_Security-Securite_Materielle CBSADSOSecurity@cbsa-asfc.gc.ca

## References

Associated Documentation





- CBSA Secure Room Guide (under revision)
- CBSA Bond Room Guide (under revision)
- CBSA Enforcement Block Guide

Links

http://www.astm.org/Standard/index.html

http://www.usg.com/content/usgcom/en_CA_east/resource-center/gypsum-construction-handbook.html

http://www.nationalgypsum.com/resources/construction-guide/NGCConstGuide.pdf

http://global.ihs.com/standards.cfm?RID=Z56A&MID=W084&selected_org=CSA&gcid=S14922X009-CSA&KEYWORD=canadian%20standards&s_kwcid=canadian%20standards|366151822

http://www.cmhc-schl.gc.ca/publications/en/rh-pr/tech/02-108.html

https://secure.spex.ca/index.php

http://www.oca.ca/

http://www.ul.com/canada/eng/pages/index.jsp

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme de conception de la sécurité matérielle

PROTECTION • SERVICE • INTÉGRITÉ

Canada



Cette norme entre en vigueur le 31 décembre 2014.

Objectif

1. L'objectif du présent document est de permettre une conception de sécurité fonctionnelle se basant sur la Gestion du risque lié à la sécurité matérielle (veuillez consulter la norme). Cette norme comprend des exigences et des recommandations.

Intention

2. L'intention du présent document est de fournir une orientation claire et concise concernant les diverses exigences incluses dans toutes les conceptions de sécurité matérielle de l'ASFC. Le document offre une conception de sécurité axée sur les objectifs avec la souplesse nécessaire pour répondre à des besoins spécifiques, tout en maintenant une norme nationale en matière de conception de sécurité matérielle. Il fournira le nécessaire pour la conception de base qui pourra s'appliquer au personnel, à l'infrastructure, aux renseignements ou aux activités.
3. Le présent document fournit des directives permettant d'assurer la conformité de l'Agence aux quatre principales considérations liées à la sécurité matérielle. Ces considérations sont les suivantes :
   a. Niveaux de protection
   b. Zones clairement visibles
   c. Concepts de protection, de détection, d'intervention et de reprise des activités,
   d. Sécurité accrue en réponse aux menaces prévisibles (jusqu'aux menaces imminentes, inclusivement) accrues ou élevées.
4. La norme sera appliquée parallèlement aux autres normes de sécurité matérielle de l'ASFC
   a. à titre de base de la Norme sur le contrôle et *surveillance de la sécurité matérielle* grâce à l'intégration de critères de mesures à la conception spécifique des contrôles;
   b. à titre de réponse à la Norme sur la *gestion du risque* en matière de la sécurité matérielle pour décrire le processus à adopter pour dans la conception de contrôles de sécurité matérielle mis en place pour traiter les questions de gestion du risque.
5. La norme a pour but de faciliter la gestion du risque lié à la sécurité grâce aux éléments suivants :
   a. Conception visant à contrôler les menaces exceptionnelles dans les espaces publics;
   b. Conception du périmètre de l'installation pour y obtenir un niveau relativement uniforme de risque résiduel,
   c. Maintien d'un contrôle approprié de l'accès, d'un niveau de protection et de systèmes de protection approprié (selon les concepts de protection, de détection, d'intervention et de reprise des activités), tout en tenant compte de toute augmentation potentielle du niveau de menace,







d. Conception de points spécifiques dans l'infrastructure (comme des salles) en fonction du risque associé à la protection du personnel, des biens et des opérations.

Portée

6. La norme concerne toutes les activités liées à l'établissement de contrôles de sécurité matérielle et autres mesures semblables dont le but est de protéger la sécurité matérielle de personnes, de biens (y compris les renseignements) et la capacité de maintenir un environnement propice aux activités.

7. La norme s'applique à toutes les infrastructures à toute étape du cycle de vie, ce qui inclut les nouvelles constructions, les rénovations et les réaménagements, peu importe l'endroit, que l'ASFC en soit le propriétaire ou un locataire.

8. La conception de la sécurité matérielle doit commencer par l'évaluation des risques. Selon le niveau de risque et la probabilité de la menace, des contrôles de sécurité seront recommandés de façon à réduire les risques matériaux à un niveau acceptable.

Application des mesures de sécurité

> *Toute évaluation des risques doit être effectuée par un expert en la matière correctement désigné selon son champ d'expertise.*

L'agent de sécurité du Ministère (ASM) et l'organisation de la sécurité sont tenus d'assurer la sécurité du personnel, des renseignements, des activités de nature délicate et des installations dans lesquelles nous menons nos activités. Le moyen le plus simple de répondre à ces obligations est d'appliquer les contrôles de sécurité matérielle de façon stratifiée.

9. La première étape est d'identifier les exigences de zonage appropriées. Les définitions et exigences concernant les zones public, d'accueil, d'activités, de sécurité et de haute sécurité sont tirées de la *Norme opérationnelle sur la sécurité matérielle (Section 6.2 – Hiérarchie des zones)*. La prochaine étape est de s'assurer qu'il y a un nombre approprié de niveaux de protection autour de ces zones.

10. Lorsqu'il est question de concevoir des niveaux de protection, le résultat du concept doit présenter, au moins, les éléments suivants :

a. Protection immédiatement autour du bien (par exemple un conteneur sécuritaire);
b. Au moins deux niveaux de protection entre celui qui protège le bien directement et le périmètre délimitant la portée du contrôle de l'Agence (par exemple une clôture délimitant la propriété). Ces niveaux de sécurité ne doivent pas présenter les mêmes faiblesses que les autres mesures en place et ne peuvent avoir recours à la même







méthode pour passer plus d'un obstacle (par exemple deux obstacles qui nécessitent la même carte d'accès ou la même pièce justificative);

c. Chaque barrière interne inclut les principes de protection, de détection, d'intervention et de reprise de sécurité décrites ci-dessous;

d. Le dernier niveau est le périmètre de contrôle qui divise l'espace où l'Agence exerce un *contrôle* des espaces où elle ne peut qu'*influencer* un certain contrôle (par exemple la limite d'une propriété).

11. Le concept de protection, de détection, d'intervention et de reprise des activités renvoie à l'utilisation des contrôles pour retarder un attaquant et l'empêcher de mener à bien son attaque jusqu'à l'arrivée des services d'intervention efficace. Ces contrôles peuvent inclure le recours à un bien ou simplement ébranler la confiance de l'attaquant en restant présent dans la zone contrôlée, sans coup férir. Ces méthodes sont décrites plus en détail dans la section sur les *niveaux de protection* ci-dessous.

12. La posture de sécurité appropriée est atteinte en adoptant les principes des niveaux de sécurité susmentionnés. Ces niveaux sont déterminés selon les points suivants :

a. la valeur du bien à protéger,

b. le milieu où les contrôles sont déployés,

c. le niveau d'assurance nécessaire pour faire en sorte que l'ensemble des contrôles de sécurité est en mesure d'empêcher une attaque.

13. En général, les contrôles de sécurité sont communiqués des façons suivantes :

a. en fonction des résultats d'une évaluation spécifique de la menace et du risque effectuée avec l'autorisation de l'ASM,

b. en fonction d'une norme établie pour une infrastructure commune, laquelle s'applique uniquement aux situations où les biens, les activités et les risques identifiés sont semblables à un point tel qu'il est impossible de les distinguer,

c. en fonction de la direction de l'ASM quelque soit le média ou la forme de communication qu'il utilise pour exercer ses pouvoirs de gestion des risques.

14. Pour qu'ils soient appropriés, les contrôles de sécurité doivent être conformes aux critères suivants ou les dépasser :

a. Ils doivent être établis en fonction d'une évaluation des risques et avoir des possibilités raisonnables d'atteindre les objectifs en matière de sécurité identifiés pour gérer le risque de sécurité.







b. Le contrôle doit pouvoir répondre aux exigences des responsables de la conception en matière de sécurité crédible. Ces responsables peuvent inclure des experts reconnus en qui renvoient à des pratiques acceptées et bien établies, des associations accréditées, des laboratoires accrédités ou des centres certifiés d'examen. Ces derniers sont souvent liés à des associations industrielles comme les *Underwriters Laboratories* ou laboratoires des assureurs (UL), etc.

c. Le contrôle doit être conforme aux exigences relatives aux lois, règlements et codes ou les dépasser.

d. Fait à noter, la Politique du gouvernement sur la sécurité et les normes des autres organismes responsables sont les normes minimales à respecter. Si l'ASFC fait face à un niveau de risque apparent accru, elle peut choisir d'aller au-delà de ces normes de références. Celles-ci ne doivent pas servir de référence pour la conception des contrôles avant qu'une évaluation des risques n'ait été effectuée et qu'Agence ait confirmé que ces normes de références sont appropriées pour l'environnement de risque identifié.

15. Les contrôles de sécurité doivent aussi être mesurables, ce qui inclut l'établissement du seuil à partir duquel on considère que la norme fonctionne comme prévu.

a. L'exigence en matière de mesure est une partie intégrale du processus de surveillance et doit être comprise dans la conception.

b. Elle doit aussi être liée à l'atténuation des risques à un niveau acceptable (selon la direction).

c. La description et la consignation des mesures doivent être conformes aux critères de vérification. Les données recueillies doivent être attestées, reproductibles et documentées correctement.

16. Les contrôles de sécurité doivent également être maintenus tout au long de leur cycle de vie. Il est important, à l'étape de la conception, de clairement l'indiquer et de tenir compte des changements opérationnels, environnementaux et des autres types de changement.

Rôles et responsabilités

17. Les experts en conception doivent inclure la conception de sécurité dans leurs plans et devis. Les agents de soumission de l'ASFC (y compris TPSGC) doivent connaître et respecter les restrictions relatives à la sécurité qui se trouvent dans le Protocole de communication et de coordination entre l'Infrastructure et la Sécurité de l'ASFC. Ils doivent faire en sorte que toutes les compagnies qui présentent une soumission répondent aux exigences relatives à la vérification d'organisation désignée (VOD) ou à la demande d'enquête de sécurité sur une organisation du secteur privé en ce qui a trait au traitement de l'information et des documents.







18. Demander d'inclure des contrôles de sécurité au processus de conception peut causer des dommages inutiles à l'infrastructure, perturber le personnel, ou engendrer des rénovations coûteuses.

19. Le Bureau de première responsabilité (BPR) et son autorité adjudicative doit faire en sorte que la Liste de vérification des exigences relatives à la sécurité, l'Énoncé des besoins, l'Énoncé des travaux, l'Énoncé de sensibilité et tout autre document présenté avant la soumission sont bien remplis et fournis au bureau de sécurité local approprié (TI et Sécurité matérielle) en vue d'y inclure les exigences relatives à la sécurité liées au contrat et de construire l'installation. Toutes les recommandations régionales doivent être approuvées par l'ASM en passant par la Direction de la sécurité et des normes professionnelles – Sécurité matérielle du Ministère.

20. La Direction générale des opérations de l'ASFC est le BPR du terrain. Elle est tenue de fournir les exigences opérationnelles, ce qui inclut un énoncé des besoins bien rempli (lequel indique clairement les espaces de travail nécessaires et, jusqu'à un certain point, leur emplacement préféré). Les autres importants documents à remplir sont les suivants :

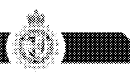
- Énoncé de sensibilité – il indique les secteurs de haute sécurité en fonction des besoins de chaque fonction de l'installation. Par exemple, l'Agence peut justifier le besoin d'une aire de discussion sécurisée ou d'une zone de haute sécurité pour des opérations classifiées.
- Liste de vérification des exigences relatives à la sécurité et l'Énoncé des travaux, sont remplis en collaboration avec Infrastructure ou l'équipe de gestion de la construction.

21. Les bureaux de sécurité régionaux sont tenus d'effectuer une évaluation de la propriété où l'installation sera construite. Ils passent en revue les dessins et les devis et établissent les exigences relatives à la sécurité en fonction de l'évaluation des risques de la propriété. Si le niveau de risque est assez faible, ils peuvent adapter les normes de base au projet. Si les niveaux de risque sont plus élevés, des mesures appropriées de sécurité accrue seront recommandées. L'ASM doit réviser et approuver toutes les résolutions.

22. La Direction de la sécurité et des normes professionnelles est responsable de l'élaboration de tous documents de directives en matière de sécurité comme les normes, les procédures, les lignes directrices, les directives et les bulletins. Elle passe en revue la sécurité matérielle de chaque installation et effectue des évaluations de la menace et du risque. Elle passe en revue tous les plans et les devis de construction pour faire en sorte que les éléments de sécurité appropriés sont en place et bien protégés, conformément au Protocole de communication et de coordination entre l'Infrastructure et la Sécurité de l'ASFC. Elle surveille la construction directement ou indirectement grâce aux rapports sur l'infrastructure et la sécurité régionale. Elle inspecte les installations en place afin de s'assurer que tous les éléments de sécurité sont présents et fonctionnels et qu'ils atténuent réellement les risques, comme prévu. Finalement, elle visite régulièrement le site pour confirmer que le profil de sécurité répond encore aux besoins en matière de sécurité.







Questions

23. Veuillez envoyer vos questions au gestionnaire de la Sécurité matérielle à l'adresse électronique suivante : CBSA-ASFC_DSO_Physical_Security-Securite_Materielle CBSADSOSecurity@cbsa-asfc.gc.ca

## Références

Documents connexes

- Guide de l'ASFC sur les pièces sécuritaires (en cours de révision)
- Guide de l'ASFC sur les locaux sous douanes (en cours de révision)
- Guide du bloc d'exécution de la loi de l'ASFC

Liens

http://www.astm.org/Standard/index.html

http://www.usg.com/content/usgcom/en_CA_east/resource-center/gypsum-construction-handbook.html

http://www.nationalgypsum.com/resources/construction-guide/NGCConstGuide.pdf

http://global.ihs.com/standards.cfm?RID=Z56A&MID=W084&selected_org=CSA&gcid=S14922X009-CSA&KEYWORD=canadian%20standards&s_kwcid=canadian%20standards|366151822

http://www.cmhc-schl.gc.ca/publications/fr/rh-pr/tech/02-108.html

https://secure.spex.ca/index.php

http://www.oca.ca/

http://site.ul.com/canada/fra-ca/pages/index.jsp

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme sur le contrôle et la surveillance de la sécurité matérielle

PROTECTION • SERVICE • INTÉGRITÉ





Cette norme entre en vigueur le 31 décembre 2014.

**Objet**

1. Cette norme fournit une orientation en ce qui concerne les activités liées au contrôle et à la surveillance du risque pour la sécurité matérielle. Elle comprend des exigences (exprimées par le verbe *devoir* à l'indicatif) et des recommandations (exprimées par le verbe *pouvoir* à l'indicatif, ou par le conditionnel des verbes *devoir* et *pouvoir*).

**Intention**

2. L'intention du présent document est de fournir des orientations claires et concises relativement aux différentes exigences du processus de contrôle et de surveillance de la sécurité matérielle à l'intention des personnes qui participent à ce qui suit :
   a. Visites d'aide technique (VAT)
   b. Rapprochements des inventaires et activités semblables
   c. Évaluations sur les lieux ou évaluations au niveau du programme de sécurité matérielle
   d. Ratissage de sécurité
   e. Inspections
   f. Vérifications
   g. Exercices d'entraînement et exercices
   h. Enquêtes administratives
3. Cette norme s'applique conjointement avec la Norme sur la gestion du risque en matière de la sécurité matérielle et de la Norme de conception de la sécurité matérielle. Ces deux normes décrivent des processus qui sont réunis en vue de fournir un élément de réponse important à la question « que faut-il contrôler ».

**Portée**

4. Cette norme se rapporte à toutes les activités où un particulier est tenu d'effectuer des examens ou de fournir une description de l'état de la sécurité matérielle et, en particulier, du niveau de risque résiduel inhérent à l'état de la sécurité matérielle de l'Agence.

**Exigences**

*Généralités*

5. Toutes les activités de contrôle et de surveillance doivent être reliées à une évaluation du risque. Lorsqu'une mesure de base a été adoptée, une partie de l'activité de contrôle et de surveillance consistera à vérifier que l'évaluation des menaces et des risques a bien été effectuée et validée quant au soutien de l'utilisation de normes de base.







6. On doit utiliser seulement des méthodes et des outils approuvés pour l'exercice des activités de contrôle et de surveillance ou d'autres évaluations du risque pour la sécurité matérielle. En ce qui a trait à ces outils, l'organe chargé de l'approbation est la Section de la sécurité matérielle (SSM) de la Direction de la sécurité et des normes professionnelles (DSNP).
7. Quiconque effectue des évaluations sur les lieux, des inspections et des vérifications doit être délégué de façon appropriée pour exercer ces activités. Lorsqu'il s'agit de visites d'aide technique (VAT) et de rapprochements d'inventaires, les employés doivent bien connaître les programmes ou les activités en cause sans être nécessairement délégués.
8. Avant que deux méthodes ou plus soient utilisées pour l'exercice des activités de contrôle et de surveillance, elles doivent être liées l'une à l'autre pour que les différentes valeurs et les différents résultats puissent être directement liés les uns aux autres avec une probabilité minimale d'interprétation fautive. C'est ce qu'on appelle souvent *une vérification de l'interopérabilité*.

**Méthodes et orientation particulière**

*Établissement des priorités*

9. En ce qui concerne les activités de contrôle, la priorité à accorder aux lieux doit être établie en fonction des deux éléments clés suivants :
    a. L'établissement de la priorité des lieux en fonction des risques pour la sécurité matérielle, qui est coordonnée par l'entremise de la Section de la sécurité matérielle (SSM), de la Direction de la sécurité et des normes professionnelles (DSNP), et de l'agent de sécurité du ministère (ASM).
    b. Le niveau du risque résiduel apparent dans ces lieux ou du risque inhérent à l'activité du programme, qui doit être fondé sur un éventail de sources d'information qui peuvent comprendre des rapports d'incident de sécurité, des rapports destinés au Centre des opérations frontalières et des rapports destinés à des programmes parallèles (tels que la santé et la sécurité au travail, les préparatifs d'urgence, les plans de continuité des activités ou la vérification selon le besoin, la disponibilité et l'applicabilité).
10. La SSM de la DSNP doit produire les outils de travail devant être utilisés par les régions et d'autres intervenants à cet égard. Ces outils doivent tenir compte des priorités communiquées de l'Agence.

*Établissement de priorités différentes pour évaluer l'exposition de l'Agence aux risques pour la sécurité matérielle*

11. Les activités d'établissement des priorités décrites plus haut se concentrent sur la gestion d'un programme axé sur le risque pour la sécurité matérielle, mais il y a des cas où l'Agence peut être exposée à une menace d'une nature précise et unique qui n'est pas nécessairement prise en compte dans le cadre de ces activités. Afin d'évaluer la question de l'établissement des priorités dans ce genre de situation, il est d'une importance primordiale que l'Agence détermine le secteur où la menace pourrait surgir.
12. La méthode à utiliser à cet égard est une combinaison des méthodes CARVER+S et MSHARPP.





a. La méthode CARVER s'entend d'une méthode où l'évaluateur utilise toute l'information au sein d'une organisation pour déterminer les points d'infrastructure particulièrement vulnérables.
b. La méthode MSHARPP s'entend d'une méthode où l'évaluateur utilise l'information et les ressources qui peuvent être raisonnablement disponibles à l'attaquant et, en tenant compte des antécédents de l'attaquant, utilise cette information pour déterminer les points d'infrastructure particulièrement vulnérables.

*Buts et objectifs des activités de contrôle*

13. L'objet des activités de contrôle et de surveillance est de réaliser les objectifs suivants dans le cadre du programme de sécurité matérielle :
    a. ***Objectif 1 – Sensibilisation à la situation*** par rapport à ce qui suit :
        i. A-t-on mis en place des contrôles de sécurité et des systèmes de protection?
        ii. Ces contrôles et ces systèmes fonctionnent-ils comme prévu?
        iii. Ces contrôles et ces systèmes ont-ils pour résultat un changement positif quant aux risques résiduels pour la sécurité matérielle?
    b. ***Objectif 2 – Contrôle de la performance*** par rapport à ce qui suit :
        i. Déterminer si des activités ou des programmes précis ou particuliers, à l'Agence, semblent courir un plus grand risque pour la sécurité matérielle.
        ii. Déterminer si des programmes précis ou particuliers montrent une tendance à l'amélioration, au maintien du statu quo ou à la régression par rapport aux décisions de la direction concernant la gestion des risques pour la sécurité matérielle.
    c. ***Objectif 3 – Aide à la gestion des risques d'entreprise*** relativement à la capacité de démontrer à la fois une gestion efficace du risque et la responsabilité à l'égard du public en matière d'affectation des ressources.
        i. L'objet de l'activité de contrôle et de surveillance est de s'assurer que les ressources engagées sont affectées conformément à l'intention de la direction et, selon les résultats découverts, de déterminer si ces mesures produisent l'effet voulu.
        ii. L'activité de contrôle et de surveillance sert aussi à suivre les progrès que fait l'Agence pour atteindre ses buts et objectifs relatifs à la sécurité matérielle et pour maintenir ses acquis.
    d. ***Objectif 4 – Détection précoce*** des défaillances, des possibilités d'amélioration et des pratiques exemplaires
        i. En déterminant les facteurs qui mènent à ce qui précède et en les communiquant à l'ensemble du programme, celui-ci peut déterminer les nouveaux enjeux, et les contrôler ou maximiser les avantages liés aux pratiques exemplaires.
14. Dans le cadre de ce programme, l'activité de contrôle et de surveillance soutient aussi l'ensemble du programme de sécurité matérielle au moyen de ce qui suit :
    a. Par la mise sur pied d'une activité d'établissement des priorités axée sur le risque et le maintien de la capacité de la lier aux objectifs de la direction en matière de contrôle, cet







effort permet de stabiliser les estimations des coûts liés à différentes activités. À cette fin, l'activité de surveillance particulière permet d'établir des objectifs mesurables (tels que le nombre des lieux visés ou les pourcentages des lieux critiques, etc.) et, à partir de la portée des activités, fournit la base pour l'affectation des ressources.

*Activités particulières de contrôle et de surveillance*

15. Les activités suivantes entrent dans le champ des activités de contrôle et de surveillance. Chacune de celles-ci est décrite en détail dans cette norme, mais peut être décrite de façon plus approfondie dans les lignes directrices pour chacun des éléments suivants :
    a. Visites d'aide technique (VAT),
    b. Évaluations sur les lieux ou évaluations de la sécurité matérielle au niveau du programme,
    c. Rapprochement d'inventaires et activités semblables,
    d. Ratissage de sécurité,
    e. Inspections,
    f. Vérifications,
    g. Exercices d'entraînement et exercices,
    h. Enquêtes administratives et criminelles.

*Activités de renforcement des capacités*

16. *Les* ***visites d'aide technique (VAT)*** servent à aider les gestionnaires locaux à répondre aux exigences liées aux buts et aux objectifs en matière de sécurité matérielle de la direction. En ce qui concerne ces visites, le gestionnaire local demande l'aide d'experts en la matière pour répondre à certaines exigences; elles sont fondées sur la disponibilité mutuelle de l'installation ou de l'organisation locale et des employés de la Sécurité matérielle. Voici une description de la façon d'effectuer une VAT en général :
    a. Le gestionnaire local détermine le sujet de préoccupation et le communique, par l'intermédiaire de la direction de la Sécurité régionale, au gestionnaire de la Sécurité matérielle.
    b. On clarifie la nature et l'étendue de l'enjeu afin de déterminer les problèmes ou les défis précis.
    c. On détermine les experts en la matière (EM) qui peuvent apporter leur aide.
    d. On entreprend des activités de coordination. Il est à noter que la VAT, qui est effectuée à la demande du gestionnaire, peut être assujettie au recouvrement des coûts.
    e. L'EM évalue le défi en fonction des pratiques et des principes acceptés par l'Agence, en collaborant avec le gestionnaire local pour trouver des solutions de rechange à la réalisation des buts et des objectifs de l'Agence.
    f. Lorsque ces mesures dérogent à la pratique courante, l'EM rédige un compte rendu des écarts avec la participation du gestionnaire local, qu'il remet au gestionnaire de la Sécurité matérielle pour que celui-ci en tienne compte lors de l'examen des politiques et des normes.







g. *Il est à noter que la durée et l'étendue des activités liées aux VAT dépendent grandement du contexte, et que le fait de parvenir à une entente mutuelle sur le niveau d'effort fait partie des activités de coordination.*

17. *Les* ***évaluations sur les lieux*** sont effectuées par des personnes déléguées et visent à déterminer si le niveau de risque résiduel dans l'installation correspond à l'attente de la direction relative au risque résiduel lié aux lieux, et on fait des recommandations sur la façon de s'assurer que les lieux évalués répondent aux attentes de la direction. Voici une description de la façon d'effectuer, en général, une évaluation sur les lieux :
    a. Les buts, les critères et les objectifs relatifs à la sécurité sont documentés en ce qui concerne les lieux;
    b. On cherche à obtenir une récente évaluation de la menace, et on la compare à l'évaluation de la menace précédente. On peut sauter cette étape lorsqu'il n'y a eu aucun changement aux opérations et aucun incident de sécurité, et que l'évaluation de la menace utilisée date de moins d'un an.
    c. On effectue la visite sur les lieux et on vérifie la performance des contrôles de la sécurité.
    d. Les résultats de la visite sur les lieux sont vérifiés par rapport au niveau de performance souhaité, lequel est défini par les critères de sécurité.
        i. Lorsque les résultats de la visite sur les lieux dépassent les attentes communiquées selon les critères de sécurité, on considère que le résultat de l'évaluation sur les lieux est « au-delà des attentes ». Lorsque le niveau de menace a augmenté, le résultat « au-delà des attentes » peut être réduit à « satisfaisant » lorsque l'augmentation de la menace correspond aux menaces prises en compte dans la détermination des objectifs et des critères de sécurité.
        ii. Lorsque les résultats de la visite sur les lieux satisfont aux attentes communiquées selon les critères de sécurité, on considère que le résultat de l'évaluation sur les lieux est « satisfaisant ». Lorsque le niveau de menace a augmenté, le résultat « satisfaisant » peut être réduit à « améliorations recommandées » lorsque l'augmentation de la menace correspond à la menace prise en compte dans la détermination des objectifs et des critères de sécurité.

18. Lorsque les résultats de la visite sur les lieux ne satisfont pas aux attentes prévues selon les critères de sécurité, on considère que le résultat de la visite sur les lieux est « améliorations recommandées ». Lorsque le niveau de la menace a augmenté, le résultat « améliorations recommandées » peut être réduit à « mesure à prendre ».

*Activités de vérification*

19. ***Le rapprochement d'inventaires*** est utilisé pour constater l'existence de biens nommément désignés. Le but de cette activité est de vérifier que les biens corporels en un lieu donné correspondent exactement à tous les dossiers d'inventaires. Voici une description de la façon d'effectuer, en général, un rapprochement d'inventaires :
    a. L'inventaire électronique du lieu examiné est imprimé à partir d'une certaine date.







b. On communique avec la direction locale afin de déterminer si des opérations supplémentaires sont susceptibles de survenir après cette date ou qu'elles sont encore en cours au moment de la vérification physique.

c. La personne responsable de l'inventaire sur les lieux prend l'inventaire électronique et constate de visu l'existence des articles en les dénombrant.

   i. Lorsqu'il manque un bien, on exige les documents officiels qui indiquent clairement l'emplacement du bien.

d. La personne chargée de l'inventaire fait signer le rapport par l'agent principal ou l'agent désigné responsable de la gestion des biens sur les lieux.

e. L'inventaire établi par suite du rapprochement (qui indique maintenant la disposition actuelle de tous les biens) est renvoyé au coordonnateur national chargé des biens contrôlés à la Section de la sécurité matérielle.

20. Les ***ratissages de sécurité*** sont effectués par le personnel délégué et visent à confirmer que les contrôles de sécurité sont en place et que le personnel fait preuve d'un niveau élémentaire de respect des exigences de sécurité dans l'établissement. Il s'agit de la forme la moins intense de vérification et, à ce titre, elle vise à établir un juste milieu entre la vérification de la conformité et l'éducation et la sensibilisation. En règle générale, le ratissage de sécurité comporte les éléments suivants :

    a. Les exigences sont communiquées à la direction du lieu faisant l'objet du ratissage de sécurité. À ce stade, la direction du lieu a l'occasion de demander des éclaircissements.

    b. On convient de la date, de l'heure et des points de coordination précis du ratissage de sécurité. La direction du site doit mettre à la disposition de l'équipe chargée du ratissage un service d'escorte qui clarifiera toute question et servira également d'escorte de sécurité au moment de passer dans les zones opérationnelles ou près de ces zones.

    c. Pendant le ratissage, l'équipe consigne les observations.

    d. Une fois le ratissage effectué, un premier mémoire est transmis à la direction du lieu ratissé. Ce mémoire doit mentionner que toutes les conclusions sont préliminaires et qu'elles doivent d'abord être examinées. Il doit également indiquer la date à laquelle la direction du lieu peut s'attendre à recevoir le rapport officiel.

21. Les ***inspections de sécurité*** représentent le niveau suivant de contrôle et de surveillance. L'inspection consiste à vérifier que tous les contrôles de sécurité sont en place, qu'ils fonctionnent tous correctement et que l'exactitude de tous les éléments communiqués peut être vérifiée.

    a. C'est la raison pour laquelle l'inspection de sécurité n'est pas considérée comme une évaluation de la sécurité, mais plutôt comme une vérification de la conformité. Il doit être clair que la conformité ne concerne pas forcément la sécurité.

    b. C'est pourquoi l'inspection de sécurité ne doit pas également être perçue comme un outil de renforcement des capacités, mais plutôt comme un outil de surveillance à la base de l'application des exigences.

22. Les ***vérifications de sécurité*** consistent non seulement à évaluer le niveau de conformité, mais aussi à évaluer que la structure de la direction, les délégations, les processus, et les décisions répondent tous aux exigences du programme de sécurité. À ce titre, elles ressemblent aux autres vérifications







internes et respectent les principes énoncés dans les normes internationales pour la pratique professionnelle de l'audit interne (*International Standard for the Professional Practice of Internal Auditing)*, de 2013.

a. Étant donné que le processus de conception en matière de sécurité matérielle repose sur l'Évaluation des menaces et des risques (EMR), la première chose à confirmer est si les exigences précises découlent du processus de l'EMR ou simplement des normes.
b. La deuxième chose consiste à établir un lien entre l'EMR et le principe de conception en matière de sécurité. Il s'agit de déterminer si les mesures précises reposent sur les résultats de l'EMR et suivent des pratiques de conception fiables ou si le processus de conception en matière de sécurité a recours aux exigences de base en matière de sécurité étant donné qu'aucun risque supplémentaire ou élevé n'a été détecté.
c. C'est uniquement après avoir effectué les deux étapes précédentes que l'on peut établir des exigences de vérification précises pour un lieu donné. Il est important de noter qu'il peut y avoir des différences d'un lieu à l'autre selon la nature des risques existants, la disponibilité des matériaux et d'autres facteurs similaires.

23. Les vérifications de sécurité peuvent également être prises en charge par la fonction de vérification interne de l'Agence. Le résultat de ces vérifications est également examiné afin d'être intégré dans l'activité de contrôle et de surveillance comme l'opinion d'une tierce partie sur l'efficacité de l'ensemble du système.

*Faire appliquer les normes*

24. Les ***incidents de sécurité*** représentent un élément important des activités de contrôle et de surveillance de l'Agence, car ils mettent en évidence les domaines sur lesquels le programme de sécurité doit mettre l'accent pour atteindre les objectifs généraux consistant à s'assurer que le personnel, les biens (y compris l'information) et les environnements opérationnels sont bien protégés.
    a. Le coordonnateur des rapports d'incident de sécurité agit en tant que point de coordination pour la réception et la distribution des rapports d'incident de sécurité. Ces directives font autorité en ce qui concerne les exigences auxquelles le processus d'établissement de rapports doit répondre en matière d'information.
    b. Le coordonnateur des rapports d'incident de sécurité agit comme le point central de distribution des comptes rendus qui découlent des rapports d'incident de sécurité.
    c. Ces rapports doivent être transmis au moyen des outils fournis par la Section de la sécurité matérielle (SSM), à moins que ces outils ne soient pas disponibles. Le rapport d'incident de sécurité doit comporter autant d'information que possible sur les éléments suivants :
        i. Tous les biens concernés, y compris les identificateurs uniques;
        ii. Toutes les personnes concernées, y compris les témoins;
        iii. La date et l'heure du signalement et de l'incident;
        iv. L'heure confirmée où l'on était en possession pour la dernière fois des biens perdus;







v. Les circonstances ayant conduit à l'incident et les recommandations pour prévenir d'autres incidents à l'avenir;
vi. Si le bien devait être retrouvé ou rapporté, un compte rendu complet de son historique et des circonstances, dans la mesure du possible, devrait être fourni. Ce compte rendu englobe les mesures prises par la sécurité.

d. La direction pourrait désigner certains incidents comme nécessitant des délais spéciaux pour le signalement ou le suivi. On les appelle des « incidents critiques relatifs à la sécurité », et il ne faut pas les confondre avec les « incidents critiques » tout court.
e. Les incidents relatifs à la sécurité font l'objet de rapports officiels qui doivent être complets et exacts. L'omission de signaler un incident et la communication délibérée de renseignements trompeurs ou incomplets sont en règle générale considérées comme des agissements à signaler à l'organisation des enquêtes visant les normes professionnelles.
f. Il doit également être clair que toute violation des lois canadiennes doit être signalée à l'organisme d'application de la loi compétent.

25. Les enquêtes administratives doivent être menées par des enquêteurs formés en la matière. La Section de la sécurité matérielle (SSM) peut apporter un soutien technique dans le cadre de ces enquêtes au cas par cas et mener des examens préliminaires pour déterminer si un incident relatif à la sécurité doit faire l'objet d'un rapport à l'étape suivante du processus d'enquête interne (aux Normes professionnelles) ou externe (aux organismes d'application de la loi).

*Autres sources de contrôle et de surveillance*

26. Les leçons tirées des exercices d'entraînement et autres exercices peuvent servir dans le cadre des activités de contrôle et de surveillance du programme de sécurité matérielle quant à la façon dont les différents objectifs, critères et points de contrôle cadrent avec la capacité d'intervention dans des périodes de risque accru.

Planification du contrôle et de la surveillance

27. Le contrôle et la surveillance se répartissent en deux activités, à savoir :
    a. le ***suivi***, c'est-à-dire le suivi de décisions visant à mettre en place des contrôles de sécurité ou à les modifier. Comme ces contrôles sont destinés à prendre des mesures en réponse à des décisions de gestion de risques, ces activités à tendance à se concentrer sur des *visites d'assistance technique* ou des *évaluations sur les lieux*.
    b. la ***maintenance***, c'est-à-dire vérifié si les contrôles de sécurité existent et s'ils sont maintenus comme prévu. Cette activité prend en règle générale la forme de ratissages, d'inspections ou de vérifications.
28. Les ***activités de suivi*** se déroulent d'habitude au cours du même exercice que la mise en place de contrôles de sécurité. C'est la raison pour laquelle les coûts liés aux activités de suivi doivent être intégrés aux coûts initiaux du projet, à savoir :
    a. les frais de déplacement comprenant environ un jour sur place;







b. des frais éventuels d'heures supplémentaires en fonction du nombre de lieux à visiter et des dates d'échéance du projet.

29. Les activités de maintenance reposent sur une méthode de planification axée sur le risque et comportent deux niveaux :
    a. le nombre d'activités (trimestrielles, semestrielles, annuelles ou autre) doit être directement lié au niveau de risque en matière de sécurité matérielle. Les installations ou les activités désignées comme étant à plus haut risque sont plus susceptibles de connaître un niveau accru de maintenance;
    b. la nature de l'activité (ratissage, inspection, vérification) dépend des conséquences éventuelles des risques ou peut reposer sur les résultats antérieurs d'autres activités de contrôle et de surveillance entreprises par l'établissement;
    c. les activités de contrôle et de surveillance ne sont pas des activités punitives. Elles visent à prendre les mesures nécessaires pour veiller à ce que les contrôles de gestion des risques relatifs à la sécurité matérielle soient en place, qu'ils fonctionnent comme souhaité et qu'ils soient maintenus.

*Coordination*

30. Les services responsables du contrôle et de la surveillance doivent s'efforcer de coordonner leurs activités de sorte qu'elles soient intégrées à d'autres activités dans l'établissement. Cette exigence n'emporte pas l'obligation de faire approuver des activités de contrôle et de surveillance par l'établissement touché ou par l'organisation concernée.
31. Lorsqu'il est prévu que ces activités se déroulent dans les régions, les gestionnaires régionaux de la sécurité doivent être consultés quant à la nature, la durée et la teneur de ces activités.
    a. Dans la mesure du possible, le personnel régional doit prendre les devants dans la coordination des activités relevant de son domaine de responsabilité administrative. Cette démarche s'applique plus particulièrement aux activités de contrôle et de surveillance pour lesquelles la portée des répercussions liées aux risques relève de ce même domaine de responsabilité.
    b. Dans le cas où les activités de contrôle et de surveillance s'étendent sur plusieurs régions, elles doivent être coordonnées par l'intermédiaire de la Section de la sécurité matérielle (SSM) à la Direction de la sécurité et des normes professionnelles (DSNP).

*Rapports*

32. Toutes les activités de contrôle et de surveillance sont consignées, notamment les renseignements suivants :
    a. les noms des personnes impliquées;
    b. les dates et heures en question;
    c. l'endroit où les endroits en cause;
    d. un récit circonstancié des activités et des observations faites;







e. des recommandations finales et les prochaines mesures nécessaires afin de maintenir la conformité ou le niveau de risque résiduel escompté.

33. Tous les rapports doivent être soumis à l'aide des outils fournis par la SSM.
34. La SSM doit recevoir une copie conforme de tous rapports concernant les activités de contrôle et de surveillance en matière de sécurité matérielle entreprises par l'Agence.
35. Tout enregistrement (visuel ou audio) doit respecter les mesures de contrôle de sécurité imposées à l'égard de ces biens ou de cette information et destinés à prévenir l'éventualité qu'une telle information échappe au contrôle de l'Agence, en fonction de la nature de l'activité de contrôle et de surveillance.
    a. Dans le cas où de l'information ou des biens de nature délicate exigeant une protection peuvent devoir être diffusés dans le domaine public, l'affaire doit être signalée à l'agent de la sécurité du ministère (ASM) et au gestionnaire principal chargé de l'analyse des répercussions potentielles.
    b. Dans le cas où de l'information de nature délicate pourrait tomber dans le domaine public à la suite d'une activité de contrôle et de surveillance, il faut d'abord consulter le coordonnateur de l'accès à l'information pour déterminer s'il est raisonnable d'espérer une exemption à l'égard de cette information. Si le coordonnateur de l'accès à l'information ne peut pas le garantir à l'Agence, alors il faut trouver une autre méthode.

*Utilité des résultats*

36. Le résultat des constatations doit être examiné par les professionnels de la sécurité concernés et le gestionnaire de la Sécurité matérielle, ou son délégué immédiat (organe d'examen). Les constatations du rapport doivent être comparées aux objectifs en matière de sécurité matérielle au moyen des critères applicables au contrôle de sécurité. Selon le résultat des constatations, il se peut que l'organe d'examen recommande les mesures suivantes :
    a. l'ajout de contrôles de sécurité afin de remédier à des vulnérabilités qui n'avaient pas été observées auparavant;
    b. la modification de contrôles de sécurité afin d'améliorer leur efficacité;
    c. la suppression de contrôles de sécurité là où ils se sont avérés inefficaces et inutiles pour protéger le personnel, les biens ou les activités pendant les périodes de risque accru;
    d. la recommandation d'une enquête dans les cas où il existe des motifs raisonnables de croire à une violation du *Code de valeurs et d'éthique* ou le signalement à un organisme d'application de la loi compétent s'il est raisonnable de croire à une violation des lois canadiennes.
37. Toutes les activités de contrôle et de surveillance sont destinées à contribuer à la gestion des risques relatifs à la sécurité matérielle et à la gestion des programmes. Elles ne visent pas à évaluer un rendement personnel ou organisationnel, bien que le résultat des constatations puisse concourir à la tenue d'une enquête ou d'une investigation globale à cette fin.

*Suivi des constatations*







38. Un rapport officiel de constatations doit être rédigé pour toutes les activités relatives aux inspections et à l'application des normes. Ce rapport doit présenter les éléments suivants :
    *a.* la méthodologie utilisée
    *b.* les contrôles précis examinés;
    *c.* l'état de ces contrôles par rapport aux attentes de la conception en matière de sécurité. Dans les cas où le contrôle ne correspond pas à la conception proposée en matière de sécurité, une évaluation visant à déterminer si le contrôle de sécurité permet d'atteindre l'objectif de sécurité;
    *d.* un plan précis de suivi qui définit clairement les mesures particulières à prendre, les personnes responsables de la prise de ces mesures, et l'échéancier des mesures à prendre;
    *e.* dans les cas où aucune mesure ne peut être prise, une méthode pour en informer la SSM et décrire toute mesure d'atténuation prise pendant que l'on résout la situation.

**Rôles et responsabilités**

39. Le comité de gestion de la haute direction en matière de sécurité donne des orientations concernant l'intention de l'Agence de gérer sa sécurité d'ensemble. Il donne, entre autres, des orientations quant au niveau et à la nature de la surveillance à appliquer.
40. L'agent de sécurité du ministère (ASM) agit à titre d'agent principal et a le pouvoir exclusif d'accepter un risque de sécurité, y compris un risque résiduel, en tant que délégué de l'administrateur général. Il lui revient entre autres la décision de mettre en place une activité de contrôle et de surveillance de niveau accru ou élevé en matière de sécurité matérielle dans un contexte particulier.
41. Le directeur de la Division de l'infrastructure et de la sécurité de l'information surveille l'activité d'évaluation et de menaces relatives à la sécurité matérielle, en veillant à ce qu'elle cadre avec l'orientation d'ensemble de l'Agence.
42. Le gestionnaire de la Sécurité matérielle agit à titre d'autorité fonctionnelle principale en ce qui a trait aux activités de contrôle et de surveillance en matière de sécurité matérielle.

**Documents de référence**

43. Cette norme relève de la Directive sur la sécurité matérielle.
44. Cette norme s'applique conjointement avec les normes supplémentaires suivantes :
    a. la Norme de conception de la sécurité matérielle
    b. la Norme pour le contrôle de l'accès
    c. la Norme visant les biens contrôlés
    d. la Norme sur la gestion du risque en matière de la sécurité matérielle

**Demande de renseignements**

45. Les demandes de renseignements doivent être transmises au gestionnaire de la Sécurité matérielle.



# Norme sur le contrôle et la surveillance de la sécurité matérielle



Cette norme entre en vigueur le 31 décembre 2014.

**Objet**

1. Cette norme fournit une orientation en ce qui concerne les activités liées au contrôle et à la surveillance du risque pour la sécurité matérielle. Elle comprend des exigences (exprimées par le verbe *devoir* à l'indicatif) et des recommandations (exprimées par le verbe *pouvoir* à l'indicatif, ou par le conditionnel des verbes *devoir* et *pouvoir*).

**Intention**

2. L'intention du présent document est de fournir des orientations claires et concises relativement aux différentes exigences du processus de contrôle et de surveillance de la sécurité matérielle à l'intention des personnes qui participent à ce qui suit :
   a. Visites d'aide technique (VAT)
   b. Rapprochements des inventaires et activités semblables
   c. Évaluations sur les lieux ou évaluations au niveau du programme de sécurité matérielle
   d. Ratissage de sécurité
   e. Inspections
   f. Vérifications
   g. Exercices d'entraînement et exercices
   h. Enquêtes administrative

3. Cette norme s'applique conjointement avec la Norme sur la gestion du risque en matière de la sécurité matérielle et de la Norme de conception de la sécurité matérielle. Ces deux normes décrivent des processus qui sont réunis en vue de fournir un élément de réponse important à la question « que faut-il contrôler ».

**Portée**

4. Cette norme se rapporte à toutes les activités où un particulier est tenu d'effectuer des examens ou de fournir une description de l'état de la sécurité matérielle et, en particulier, du niveau de risque résiduel inhérent à l'état de la sécurité matérielle de l'Agence.

**Exigences**

*Généralités*

5. Toutes les activités de contrôle et de surveillance doivent être reliées à une évaluation du risque. Lorsqu'une mesure de base a été adoptée, une partie de l'activité de contrôle et de surveillance







consistera à vérifier que l'évaluation des menaces et des risques a bien été effectuée et validée quant au soutien de l'utilisation de normes de base.

6. On doit utiliser seulement des méthodes et des outils approuvés pour l'exercice des activités de contrôle et de surveillance ou d'autres évaluations du risque pour la sécurité matérielle. En ce qui a trait à ces outils, l'organe chargé de l'approbation est la Section de la sécurité matérielle (SSM) de la Direction de la sécurité et des normes professionnelles (DSNP).
7. Quiconque effectue des évaluations sur les lieux, des inspections et des vérifications doit être délégué de façon appropriée pour exercer ces activités. Lorsqu'il s'agit de visites d'aide technique (VAT) et de rapprochements d'inventaires, les employés doivent bien connaître les programmes ou les activités en cause sans être nécessairement délégués.
8. Avant que deux méthodes ou plus soient utilisées pour l'exercice des activités de contrôle et de surveillance, elles doivent être liées l'une à l'autre pour que les différentes valeurs et les différents résultats puissent être directement liés les uns aux autres avec une probabilité minimale d'interprétation fautive. C'est ce qu'on appelle souvent *une vérification de l'interopérabilité*.

**Méthodes et orientation particulière**

*Établissement des priorités*

9. En ce qui concerne les activités de contrôle, la priorité à accorder aux lieux doit être établie en fonction des deux éléments clés suivants :
    a. L'établissement de la priorité des lieux en fonction des risques pour la sécurité matérielle, qui est coordonnée par l'entremise de la Section de la sécurité matérielle (SSM), de la Direction de la sécurité et des normes professionnelles (DSNP), et de l'agent de sécurité du ministère (ASM).
    b. Le niveau du risque résiduel apparent dans ces lieux ou du risque inhérent à l'activité du programme, qui doit être fondé sur un éventail de sources d'information qui peuvent comprendre des rapports d'incident de sécurité, des rapports destinés au Centre des opérations frontalières et des rapports destinés à des programmes parallèles (tels que la santé et la sécurité au travail, les préparatifs d'urgence, les plans de continuité des activités ou la vérification selon le besoin, la disponibilité et l'applicabilité).
10. La SSM de la DSNP doit produire les outils de travail devant être utilisés par les régions et d'autres intervenants à cet égard. Ces outils doivent tenir compte des priorités communiquées de l'Agence.

*Établissement de priorités différentes pour évaluer l'exposition de l'Agence aux risques pour la sécurité matérielle*

11. Les activités d'établissement des priorités décrites plus haut se concentrent sur la gestion d'un programme axé sur le risque pour la sécurité matérielle, mais il y a des cas où l'Agence peut être exposée à une menace d'une nature précise et unique qui n'est pas nécessairement prise en compte dans le cadre de ces activités. Afin d'évaluer la question de l'établissement des priorités dans ce







genre de situation, il est d'une importance primordiale que l'Agence détermine le secteur où la menace pourrait surgir.

12. La méthode à utiliser à cet égard est une combinaison des méthodes CARVER+S et MSHARPP.
    a. La méthode CARVER s'entend d'une méthode où l'évaluateur utilise toute l'information au sein d'une organisation pour déterminer les points d'infrastructure particulièrement vulnérables.
    b. La méthode MSHARPP s'entend d'une méthode où l'évaluateur utilise l'information et les ressources qui peuvent être raisonnablement disponibles à l'attaquant et, en tenant compte des antécédents de l'attaquant, utilise cette information pour déterminer les points d'infrastructure particulièrement vulnérables.

*Buts et objectifs des activités de contrôle*

13. L'objet des activités de contrôle et de surveillance est de réaliser les objectifs suivants dans le cadre du programme de sécurité matérielle :
    a. ***Objectif 1 – Sensibilisation à la situation*** par rapport à ce qui suit :
        i. A-t-on mis en place des contrôles de sécurité et des systèmes de protection?
        ii. Ces contrôles et ces systèmes fonctionnent-ils comme prévu?
        iii. Ces contrôles et ces systèmes ont-ils pour résultat un changement positif quant aux risques résiduels pour la sécurité matérielle?
    b. ***Objectif 2 – Contrôle de la performance*** par rapport à ce qui suit :
        i. Déterminer si des activités ou des programmes précis ou particuliers, à l'Agence, semblent courir un plus grand risque pour la sécurité matérielle.
        ii. Déterminer si des programmes précis ou particuliers montrent une tendance à l'amélioration, au maintien du statu quo ou à la régression par rapport aux décisions de la direction concernant la gestion des risques pour la sécurité matérielle.
    c. ***Objectif 3 – Aide à la gestion des risques d'entreprise*** relativement à la capacité de démontrer à la fois une gestion efficace du risque et la responsabilité à l'égard du public en matière d'affectation des ressources.
        i. L'objet de l'activité de contrôle et de surveillance est de s'assurer que les ressources engagées sont affectées conformément à l'intention de la direction et, selon les résultats découverts, de déterminer si ces mesures produisent l'effet voulu.
        ii. L'activité de contrôle et de surveillance sert aussi à suivre les progrès que fait l'Agence pour atteindre ses buts et objectifs relatifs à la sécurité matérielle et pour maintenir ses acquis.
    d. ***Objectif 4 – Détection précoce*** des défaillances, des possibilités d'amélioration et des pratiques exemplaires
        i. En déterminant les facteurs qui mènent à ce qui précède et en les communiquant à l'ensemble du programme, celui-ci peut déterminer les nouveaux enjeux, et les contrôler ou maximiser les avantages liés aux pratiques exemplaires.







14. Dans le cadre de ce programme, l'activité de contrôle et de surveillance soutient aussi l'ensemble du programme de sécurité matérielle au moyen de ce qui suit :
    a. Par la mise sur pied d'une activité d'établissement des priorités axée sur le risque et le maintien de la capacité de la lier aux objectifs de la direction en matière de contrôle, cet effort permet de stabiliser les estimations des coûts liés à différentes activités. À cette fin, l'activité de surveillance particulière permet d'établir des objectifs mesurables (tels que le nombre des lieux visés ou les pourcentages des lieux critiques, etc.) et, à partir de la portée des activités, fournit la base pour l'affectation des ressources.

*Activités particulières de contrôle et de surveillance*

15. Les activités suivantes entrent dans le champ des activités de contrôle et de surveillance. Chacune de celles-ci est décrite en détail dans cette norme, mais peut être décrite de façon plus approfondie dans les lignes directrices pour chacun des éléments suivants :
    a. Visites d'aide technique (VAT),
    b. Évaluations sur les lieux ou évaluations de la sécurité matérielle au niveau du programme,
    c. Rapprochement d'inventaires et activités semblables,
    d. Ratissage de sécurité,
    e. Inspections,
    f. Vérifications,
    g. Exercices d'entraînement et exercices,
    h. Enquêtes administratives et criminelles.

*Activités de renforcement des capacités*

16. *Les* ***visites d'aide technique (VAT)*** servent à aider les gestionnaires locaux à répondre aux exigences liées aux buts et aux objectifs en matière de sécurité matérielle de la direction. En ce qui concerne ces visites, le gestionnaire local demande l'aide d'experts en la matière pour répondre à certaines exigences; elles sont fondées sur la disponibilité mutuelle de l'installation ou de l'organisation locale et des employés de la Sécurité matérielle. Voici une description de la façon d'effectuer une VAT en général :
    a. Le gestionnaire local détermine le sujet de préoccupation et le communique, par l'intermédiaire de la direction de la Sécurité régionale, au gestionnaire de la Sécurité matérielle.
    b. On clarifie la nature et l'étendue de l'enjeu afin de déterminer les problèmes ou les défis précis.
    c. On détermine les experts en la matière (EM) qui peuvent apporter leur aide.
    d. On entreprend des activités de coordination. Il est à noter que la VAT, qui est effectuée à la demande du gestionnaire, peut être assujettie au recouvrement des coûts.



e. L'EM évalue le défi en fonction des pratiques et des principes acceptés par l'Agence, en collaborant avec le gestionnaire local pour trouver des solutions de rechange à la réalisation des buts et des objectifs de l'Agence.
f. Lorsque ces mesures dérogent à la pratique courante, l'EM rédige un compte rendu des écarts avec la participation du gestionnaire local, qu'il remet au gestionnaire de la Sécurité matérielle pour que celui-ci en tienne compte lors de l'examen des politiques et des normes.
g. *Il est à noter que la durée et l'étendue des activités liées aux VAT dépendent grandement du contexte, et que le fait de parvenir à une entente mutuelle sur le niveau d'effort fait partie des activités de coordination.*

17. *Les* ***évaluations sur les lieux*** sont effectuées par des personnes déléguées et visent à déterminer si le niveau de risque résiduel dans l'installation correspond à l'attente de la direction relative au risque résiduel lié aux lieux, et on fait des recommandations sur la façon de s'assurer que les lieux évalués répondent aux attentes de la direction. Voici une description de la façon d'effectuer, en général, une évaluation sur les lieux :
    a. Les buts, les critères et les objectifs relatifs à la sécurité sont documentés en ce qui concerne les lieux;
    b. On cherche à obtenir une récente évaluation de la menace, et on la compare à l'évaluation de la menace précédente. On peut sauter cette étape lorsqu'il n'y a eu aucun changement aux opérations et aucun incident de sécurité, et que l'évaluation de la menace utilisée date de moins d'un an.
    c. On effectue la visite sur les lieux et on vérifie la performance des contrôles de la sécurité.
    d. Les résultats de la visite sur les lieux sont vérifiés par rapport au niveau de performance souhaité, lequel est défini par les critères de sécurité.
        i. Lorsque les résultats de la visite sur les lieux dépassent les attentes communiquées selon les critères de sécurité, on considère que le résultat de l'évaluation sur les lieux est « au-delà des attentes ». Lorsque le niveau de menace a augmenté, le résultat « au-delà des attentes » peut être réduit à « satisfaisant » lorsque l'augmentation de la menace correspond aux menaces prises en compte dans la détermination des objectifs et des critères de sécurité.
        ii. Lorsque les résultats de la visite sur les lieux satisfont aux attentes communiquées selon les critères de sécurité, on considère que le résultat de l'évaluation sur les lieux est « satisfaisant ». Lorsque le niveau de menace a augmenté, le résultat « satisfaisant » peut être réduit à « améliorations recommandées » lorsque l'augmentation de la menace correspond à la menace prise en compte dans la détermination des objectifs et des critères de sécurité.
18. Lorsque les résultats de la visite sur les lieux ne satisfont pas aux attentes prévues selon les critères de sécurité, on considère que le résultat de la visite sur les lieux est « améliorations recommandées ». Lorsque le niveau de la menace a augmenté, le résultat « améliorations recommandées » peut être réduit à « mesure à prendre ».



*Activités de vérification*

19. ***Le rapprochement d'inventaires*** est utilisé pour constater l'existence de biens nommément désignés. Le but de cette activité est de vérifier que les biens corporels en un lieu donné correspondent exactement à tous les dossiers d'inventaires. Voici une description de la façon d'effectuer, en général, un rapprochement d'inventaires :
    a. L'inventaire électronique du lieu examiné est imprimé à partir d'une certaine date.
    b. On communique avec la direction locale afin de déterminer si des opérations supplémentaires sont susceptibles de survenir après cette date ou qu'elles sont encore en cours au moment de la vérification physique.
    c. La personne responsable de l'inventaire sur les lieux prend l'inventaire électronique et constate de visu l'existence des articles en les dénombrant.
        i. Lorsqu'il manque un bien, on exige les documents officiels qui indiquent clairement l'emplacement du bien.
    d. La personne chargée de l'inventaire fait signer le rapport par l'agent principal ou l'agent désigné responsable de la gestion des biens sur les lieux.
    e. L'inventaire établi par suite du rapprochement (qui indique maintenant la disposition actuelle de tous les biens) est renvoyé au coordonnateur national chargé des biens contrôlés à la Section de la sécurité matérielle.
20. Les ***ratissages de sécurité*** sont effectués par le personnel délégué et visent à confirmer que les contrôles de sécurité sont en place et que le personnel fait preuve d'un niveau élémentaire de respect des exigences de sécurité dans l'établissement. Il s'agit de la forme la moins intense de vérification et, à ce titre, elle vise à établir un juste milieu entre la vérification de la conformité et l'éducation et la sensibilisation. En règle générale, le ratissage de sécurité comporte les éléments suivants :
    a. Les exigences sont communiquées à la direction du lieu faisant l'objet du ratissage de sécurité. À ce stade, la direction du lieu a l'occasion de demander des éclaircissements.
    b. On convient de la date, de l'heure et des points de coordination précis du ratissage de sécurité. La direction du site doit mettre à la disposition de l'équipe chargée du ratissage un service d'escorte qui clarifiera toute question et servira également d'escorte de sécurité au moment de passer dans les zones opérationnelles ou près de ces zones.
    c. Pendant le ratissage, l'équipe consigne les observations.
    d. Une fois le ratissage effectué, un premier mémoire est transmis à la direction du lieu ratissé. Ce mémoire doit mentionner que toutes les conclusions sont préliminaires et qu'elles doivent d'abord être examinées. Il doit également indiquer la date à laquelle la direction du lieu peut s'attendre à recevoir le rapport officiel.
21. Les ***inspections de sécurité*** représentent le niveau suivant de contrôle et de surveillance. L'inspection consiste à vérifier que tous les contrôles de sécurité sont en place, qu'ils fonctionnent tous correctement et que l'exactitude de tous les éléments communiqués peut être vérifiée.







a. C'est la raison pour laquelle l'inspection de sécurité n'est pas considérée comme une évaluation de la sécurité, mais plutôt comme une vérification de la conformité. Il doit être clair que la conformité ne concerne pas forcément la sécurité.
b. C'est pourquoi l'inspection de sécurité ne doit pas également être perçue comme un outil de renforcement des capacités, mais plutôt comme un outil de surveillance à la base de l'application des exigences.

22. Les ***vérifications de sécurité*** consistent non seulement à évaluer le niveau de conformité, mais aussi à évaluer que la structure de la direction, les délégations, les processus, et les décisions répondent tous aux exigences du programme de sécurité. À ce titre, elles ressemblent aux autres vérifications internes et respectent les principes énoncés dans les normes internationales pour la pratique professionnelle de l'audit interne (*International Standard for the Professional Practice of Internal Auditing)*, de 2013.
    a. Étant donné que le processus de conception en matière de sécurité matérielle repose sur l'Évaluation des menaces et des risques (EMR), la première chose à confirmer est si les exigences précises découlent du processus de l'EMR ou simplement des normes.
    b. La deuxième chose consiste à établir un lien entre l'EMR et le principe de conception en matière de sécurité. Il s'agit de déterminer si les mesures précises reposent sur les résultats de l'EMR et suivent des pratiques de conception fiables ou si le processus de conception en matière de sécurité a recours aux exigences de base en matière de sécurité étant donné qu'aucun risque supplémentaire ou élevé n'a été détecté.
    c. C'est uniquement après avoir effectué les deux étapes précédentes que l'on peut établir des exigences de vérification précises pour un lieu donné. Il est important de noter qu'il peut y avoir des différences d'un lieu à l'autre selon la nature des risques existants, la disponibilité des matériaux et d'autres facteurs similaires.
23. Les vérifications de sécurité peuvent également être prises en charge par la fonction de vérification interne de l'Agence. Le résultat de ces vérifications est également examiné afin d'être intégré dans l'activité de contrôle et de surveillance comme l'opinion d'une tierce partie sur l'efficacité de l'ensemble du système.

*Faire appliquer les normes*

24. Les ***incidents de sécurité*** représentent un élément important des activités de contrôle et de surveillance de l'Agence, car ils mettent en évidence les domaines sur lesquels le programme de sécurité doit mettre l'accent pour atteindre les objectifs généraux consistant à s'assurer que le personnel, les biens (y compris l'information) et les environnements opérationnels sont bien protégés.
    a. Le coordonnateur des rapports d'incident de sécurité agit en tant que point de coordination pour la réception et la distribution des rapports d'incident de sécurité. Ces directives font autorité en ce qui concerne les exigences auxquelles le processus d'établissement de rapports doit répondre en matière d'information.







b. Le coordonnateur des rapports d'incident de sécurité agit comme le point central de distribution des comptes rendus qui découlent des rapports d'incident de sécurité.

c. Ces rapports doivent être transmis au moyen des outils fournis par la Section de la sécurité matérielle (SSM), à moins que ces outils ne soient pas disponibles. Le rapport d'incident de sécurité doit comporter autant d'information que possible sur les éléments suivants :
   i. Tous les biens concernés, y compris les identificateurs uniques;
   ii. Toutes les personnes concernées, y compris les témoins;
   iii. La date et l'heure du signalement et de l'incident;
   iv. L'heure confirmée où l'on était en possession pour la dernière fois des biens perdus;
   v. Les circonstances ayant conduit à l'incident et les recommandations pour prévenir d'autres incidents à l'avenir;
   vi. Si le bien devait être retrouvé ou rapporté, un compte rendu complet de son historique et des circonstances, dans la mesure du possible, devrait être fourni. Ce compte rendu englobe les mesures prises par la sécurité.

d. La direction pourrait désigner certains incidents comme nécessitant des délais spéciaux pour le signalement ou le suivi. On les appelle des « incidents critiques relatifs à la sécurité », et il ne faut pas les confondre avec les « incidents critiques » tout court.

e. Les incidents relatifs à la sécurité font l'objet de rapports officiels qui doivent être complets et exacts. L'omission de signaler un incident et la communication délibérée de renseignements trompeurs ou incomplets sont en règle générale considérées comme des agissements à signaler à l'organisation des enquêtes visant les normes professionnelles.

f. Il doit également être clair que toute violation des lois canadiennes doit être signalée à l'organisme d'application de la loi compétent.

25. Les enquêtes administratives doivent être menées par des enquêteurs formés en la matière. La Section de la sécurité matérielle (SSM) peut apporter un soutien technique dans le cadre de ces enquêtes au cas par cas et mener des examens préliminaires pour déterminer si un incident relatif à la sécurité doit faire l'objet d'un rapport à l'étape suivante du processus d'enquête interne (aux Normes professionnelles) ou externe (aux organismes d'application de la loi).

*Autres sources de contrôle et de surveillance*

26. Les leçons tirées des exercices d'entraînement et autres exercices peuvent servir dans le cadre des activités de contrôle et de surveillance du programme de sécurité matérielle quant à la façon dont les différents objectifs, critères et points de contrôle cadrent avec la capacité d'intervention dans des périodes de risque accru.

Planification du contrôle et de la surveillance

27. Le contrôle et la surveillance se répartissent en deux activités, à savoir :
   a. le ***suivi***, c'est-à-dire le suivi de décisions visant à mettre en place des contrôles de sécurité ou à les modifier. Comme ces contrôles sont destinés à prendre des mesures en réponse à



des décisions de gestion de risques, ces activités à tendance à se concentrer sur des *visites d'assistance technique* ou des *évaluations sur les lieux*.

b. la ***maintenance***, c'est-à-dire vérifié si les contrôles de sécurité existent et s'ils sont maintenus comme prévu. Cette activité prend en règle générale la forme de ratissages, d'inspections ou de vérifications.

28. Les ***activités de suivi*** se déroulent d'habitude au cours du même exercice que la mise en place de contrôles de sécurité. C'est la raison pour laquelle les coûts liés aux activités de suivi doivent être intégrés aux coûts initiaux du projet, à savoir :
    a. les frais de déplacement comprenant environ un jour sur place;
    b. des frais éventuels d'heures supplémentaires en fonction du nombre de lieux à visiter et des dates d'échéance du projet.
29. Les activités de maintenance reposent sur une méthode de planification axée sur le risque et comportent deux niveaux :
    a. le nombre d'activités (trimestrielles, semestrielles, annuelles ou autre) doit être directement lié au niveau de risque en matière de sécurité matérielle. Les installations ou les activités désignées comme étant à plus haut risque sont plus susceptibles de connaître un niveau accru de maintenance;
    b. la nature de l'activité (ratissage, inspection, vérification) dépend des conséquences éventuelles des risques ou peut reposer sur les résultats antérieurs d'autres activités de contrôle et de surveillance entreprises par l'établissement;
    c. les activités de contrôle et de surveillance ne sont pas des activités punitives. Elles visent à prendre les mesures nécessaires pour veiller à ce que les contrôles de gestion des risques relatifs à la sécurité matérielle soient en place, qu'ils fonctionnent comme souhaité et qu'ils soient maintenus.

*Coordination*

30. Les services responsables du contrôle et de la surveillance doivent s'efforcer de coordonner leurs activités de sorte qu'elles soient intégrées à d'autres activités dans l'établissement. Cette exigence n'emporte pas l'obligation de faire approuver des activités de contrôle et de surveillance par l'établissement touché ou par l'organisation concernée.
31. Lorsqu'il est prévu que ces activités se déroulent dans les régions, les gestionnaires régionaux de la sécurité doivent être consultés quant à la nature, la durée et la teneur de ces activités.
    a. Dans la mesure du possible, le personnel régional doit prendre les devants dans la coordination des activités relevant de son domaine de responsabilité administrative. Cette démarche s'applique plus particulièrement aux activités de contrôle et de surveillance pour lesquelles la portée des répercussions liées aux risques relève de ce même domaine de responsabilité.



b. Dans le cas où les activités de contrôle et de surveillance s'étendent sur plusieurs régions, elles doivent être coordonnées par l'intermédiaire de la Section de la sécurité matérielle (SSM) à la Direction de la sécurité et des normes professionnelles (DSNP).

*Rapports*

32. Toutes les activités de contrôle et de surveillance sont consignées, notamment les renseignements suivants :
    a. les noms des personnes impliquées;
    b. les dates et heures en question;
    c. l'endroit où les endroits en cause;
    d. un récit circonstancié des activités et des observations faites;
    e. des recommandations finales et les prochaines mesures nécessaires afin de maintenir la conformité ou le niveau de risque résiduel escompté.
33. Tous les rapports doivent être soumis à l'aide des outils fournis par la SSM.
34. La SSM doit recevoir une copie conforme de tous rapports concernant les activités de contrôle et de surveillance en matière de sécurité matérielle entreprises par l'Agence.
35. Tout enregistrement (visuel ou audio) doit respecter les mesures de contrôle de sécurité imposées à l'égard de ces biens ou de cette information et destinés à prévenir l'éventualité qu'une telle information échappe au contrôle de l'Agence, en fonction de la nature de l'activité de contrôle et de surveillance.
    a. Dans le cas où de l'information ou des biens de nature délicate exigeant une protection peuvent devoir être diffusés dans le domaine public, l'affaire doit être signalée à l'agent de la sécurité du ministère (ASM) et au gestionnaire principal chargé de l'analyse des répercussions potentielles.
    b. Dans le cas où de l'information de nature délicate pourrait tomber dans le domaine public à la suite d'une activité de contrôle et de surveillance, il faut d'abord consulter le coordonnateur de l'accès à l'information pour déterminer s'il est raisonnable d'espérer une exemption à l'égard de cette information. Si le coordonnateur de l'accès à l'information ne peut pas le garantir à l'Agence, alors il faut trouver une autre méthode.

*Utilité des résultats*

36. Le résultat des constatations doit être examiné par les professionnels de la sécurité concernés et le gestionnaire de la Sécurité matérielle, ou son délégué immédiat (organe d'examen). Les constatations du rapport doivent être comparées aux objectifs en matière de sécurité matérielle au moyen des critères applicables au contrôle de sécurité. Selon le résultat des constatations, il se peut que l'organe d'examen recommande les mesures suivantes :
    a. l'ajout de contrôles de sécurité afin de remédier à des vulnérabilités qui n'avaient pas été observées auparavant;
    b. la modification de contrôles de sécurité afin d'améliorer leur efficacité;





c. la suppression de contrôles de sécurité là où ils se sont avérés inefficaces et inutiles pour protéger le personnel, les biens ou les activités pendant les périodes de risque accru;
d. la recommandation d'une enquête dans les cas où il existe des motifs raisonnables de croire à une violation du *Code de valeurs et d'éthique* ou le signalement à un organisme d'application de la loi compétent s'il est raisonnable de croire à une violation des lois canadiennes.

37. Toutes les activités de contrôle et de surveillance sont destinées à contribuer à la gestion des risques relatifs à la sécurité matérielle et à la gestion des programmes. Elles ne visent pas à évaluer un rendement personnel ou organisationnel, bien que le résultat des constatations puisse concourir à la tenue d'une enquête ou d'une investigation globale à cette fin.

*Suivi des constatations*

38. Un rapport officiel de constatations doit être rédigé pour toutes les activités relatives aux inspections et à l'application des normes. Ce rapport doit présenter les éléments suivants :
    *a.* la méthodologie utilisée
    *b.* les contrôles précis examinés;
    *c.* l'état de ces contrôles par rapport aux attentes de la conception en matière de sécurité. Dans les cas où le contrôle ne correspond pas à la conception proposée en matière de sécurité, une évaluation visant à déterminer si le contrôle de sécurité permet d'atteindre l'objectif de sécurité;
    *d.* un plan précis de suivi qui définit clairement les mesures particulières à prendre, les personnes responsables de la prise de ces mesures, et l'échéancier des mesures à prendre;
    *e.* dans les cas où aucune mesure ne peut être prise, une méthode pour en informer la SSM et décrire toute mesure d'atténuation prise pendant que l'on résout la situation.

**Rôles et responsabilités**

39. Le comité de gestion de la haute direction en matière de sécurité donne des orientations concernant l'intention de l'Agence de gérer sa sécurité d'ensemble. Il donne, entre autres, des orientations quant au niveau et à la nature de la surveillance à appliquer.
40. L'agent de sécurité du ministère (ASM) agit à titre d'agent principal et a le pouvoir exclusif d'accepter un risque de sécurité, y compris un risque résiduel, en tant que délégué de l'administrateur général. Il lui revient entre autres la décision de mettre en place une activité de contrôle et de surveillance de niveau accru ou élevé en matière de sécurité matérielle dans un contexte particulier.
41. Le directeur de la Division de l'infrastructure et de la sécurité de l'information surveille l'activité d'évaluation et de menaces relatives à la sécurité matérielle, en veillant à ce qu'elle cadre avec l'orientation d'ensemble de l'Agence.
42. Le gestionnaire de la Sécurité matérielle agit à titre d'autorité fonctionnelle principale en ce qui a trait aux activités de contrôle et de surveillance en matière de sécurité matérielle.

**Documents de référence**

43. Cette norme relève de la Directive sur la sécurité matérielle.
44. Cette norme s'applique conjointement avec les normes supplémentaires suivantes :
    a. la Norme de conception de la sécurité matérielle
    b. la Norme pour le contrôle de l'accès
    c. la Norme visant les biens contrôlés
    d. la Norme sur la gestion du risque en matière de la sécurité matérielle

**Demande de renseignements**

45. Les demandes de renseignements doivent être transmises au gestionnaire de la Sécurité matérielle.

Canada Border Services Agency
Agence des services frontaliers du Canada



# Standard for Access Control

PROTECTION • SERVICE • INTEGRITY



Canada Border Services Agency | Agence des services frontaliers du Canada



# Table of Contents



This standard takes effect on February 2, 2015.

## Purpose

1. The purpose of this standard is to provide clear, concise and comprehensive guidance on the requirements for Access Control. This document contains both requirements (indicated by must, shall, or will) and recommendations (indicated by may, should or might).

## Intent

2. The intent of the Access Control standard is to describe the conditions under which access to sensitive assets (including information) may be granted.

## Scope

3. This standard applies to all situations where any person is being proposed to have access to, or is being given access to, sensitive assets.
   a. The term "assets" is defined in terms of the definition put forward by the Treasury Board of Canada Secretariat.
   b. The term "access" is defined in terms of the individual being given custody, care, or control (even if only for a short period) in such a way that the means or opportunity to cause injury to the asset increases.
   c. This standard applies to all persons, regardless of employment status, who may be given access to sensitive assets.
   d. Where specialized rooms are involved, this Operational Standard is to be read in conjunction with the requirements associated with those spaces or environments. These include, but are not limited to: enforcement blocks guideline, arming room guidelines, communications space guidelines, secure space guidelines, etc. These additional guidelines refine the requirements communicated here to apply more completely in those environments. Note: They are Protected B and will be provided to CBSA cleared security personnel on an "AS NEED TO KNOW" basis.

## Requirements

### Governance

4. Where the Agency shares space or occupies space within another entity, the access control system for the Agency must be able to demonstrate full separation and control. Measures and their oversight / operations are to be agreed upon and clearly documented within an Occupancy Instrument (or similar mechanism) which includes the following:







  a. The delineation between base building controls maintained by Public Works or Shared Services Canada and the controls maintained by the Agency,
  b. The nature of controls in place to ensure that the CBSA retains control over its space, including any changes to the system, authorities within the system, the maintenance of the system or other controls that may influence the ability to grant access to CBSA spaces; and
  c. The mechanism by which the agreement will be monitored and overseen, including reporting requirements and the frequency and attendance requirements of any meetings associated with its operations.
5. A copy of any such agreement is to be provided to the DSO through the regional security organization.
6. Access control logs are to be maintained for all systems. Such logs are subject to the following restrictions:
  a. Personal information (such as images) is provided for the purposes of identifying individuals and controlling access. Such information is not to be used for other purposes except in circumstances where the person to whom that information applies gives clear and informed consent;
  b. Access control logs pertaining to routinely occupied spaces (such as working floors) may be made available for Professional Standards Investigations but are not to be used in terms of routine supervision,
  c. An access list to the space may be used to compare the lists of those who management has authorized to be granted access and those that have access permissions within the access control systems, and
  d. Access control logs pertaining to unoccupied spaces or special storage spaces normally not occupied by personnel may be used as the means of monitoring access; as such monitoring is associated with the detection of unauthorized entry and not the monitoring of employee performance.

## General Conditions for Granting Access

7. In order to be given routine or unescorted access to CBSA controlled spaces, the individual must be able to demonstrate that he or she has the following:
  a. A need for access in order to complete Agency-related tasks or other work, and
  b. A valid security screening granted at a level commensurate to the highest level of sensitivity that may be accessed.
8. The need for access is based on the specific assets that need to be available to the individual in order to perform his or her work. Generally, access will be limited to those spaces or assets that the employee needs in order to meet Agency expectations regarding his or her work.
9. The level of security screening associated with access is based upon the highest level of sensitivity, taking into account the following:
  a. The specific asset and its level of sensitivity;
  b. Any assets (including information) that may become available when the individual is granted access to that specific asset; and







c. Any assets (including spaces and information) to which the individual may become deliberately or accidentally exposed when in the spaces holding the specific asset.

**For example, an individual that is being given access to a computer (PROTECTED B network) in an area which routinely handles SECRET information would require a SECRET security clearance due to the potential exposure to classified information.*

10. Access must take into account the ownership of the asset, including the following:
    a. Any legal or regulatory requirements associated with the asset,
    b. Any certification or accreditation requirements associated with the asset,
    c. Any agreements (such as memoranda of understanding) associated with the asset,
    d. Any internal policy decisions, and
    e. Any contractual arrangements that must be maintained.
11. Where access is required on a temporary basis (not routine), then the individual being proposed must be *escorted* in order to afford that temporary access. This must take into account the following:
    a. The need to be given access must be clearly demonstrable and based upon work authorized by the Agency,
    b. The individual acting as escort must be acting on behalf of the Agency, possess the ability to detect unauthorized or inappropriate action, and must be committed to ensuring that an appropriate response is triggered or taken should such activity be detected.
    c. When escorting an individual, the escort must be able to attest that the individual being escorted was under constant and consistent supervision.
12. Those who have been issued a token (such as an Access Badge) must wear that badge visibly at all times when within the spaces controlled by that access unless the following applies:
    a. The wearing of such a token is contrary to the design of personal protective equipment and the uniformed officer is able to produce the token upon demand at any time within the space or in the process of gaining access to such space,
    b. The wearing of such a token puts the employee at risk in terms of occupational health and safety. Where such a claim is made, it must be made in writing, include comments by the local Occupational Health and Safety Committee including the basis for the claims, and
    c. The wearing of such token provides no intrinsic value in that the space controlled is occupied by a single group, does not allow outside personnel (including support services) into the space, does not accept visitors and does not have a high rate of staff turnover (such as assignments or secondments). In these cases, there must be a clearly defined and communicated management process that identifies to staff that is authorized to enter and any cessation of duties that reduces or eliminates the need for access. This is intended for officers deployed on vessels or equivalent circumstances.

### General Requirements Pertaining to All Access Controls

13. Where systems are used to control access, the following requirements must be met:



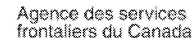




a. The system must be configured or managed in such a way that the primary control over CBSA spaces resides within the Agency,
b. The system must be configured or managed in such a way that any supporting services are not given an opportunity to grant access, manipulate the levels of access being granted or change logs associated with the levels of access granted (including to whom access has been granted);
c. The system must be configured in such a way that access is maintained and controlled on an individual level (such as through the use of a swipe card issued to an individual),
d. When considering the level of protection for the access control system, the principle of "locks and keys" applies. The level of protection to be applied to the access control system is as per the highest level of sensitivity of asset that it protects.

14. In the design of access control measures, the following design criteria must be implemented and maintained:
    a. ***Preventive*** controls that ensure that all those seeking access must proceed through the Agency-authorized (including security approval) means of being granted appropriate access,
    b. ***Detection*** methods that include both the ability to detect attempts to bypass the above controls physically (such as through breaching the perimeter) or administratively (in terms of making false claims on access control requests),
    c. An effective ***response*** in terms of either an internal response using Agency personnel (as appropriate) or outside services contracted for that purpose and meeting the security requirements to themselves having access, and
    d. A plan, periodically reviewed and tested, to address predictable situations where the access control system is determined or reasonably believed to have failed and to re-establish trust in the system (***recovery***).

15. When occupying space in shared spaces and where access for first responders or emergency personnel is required, the following steps are to be taken:
    a. The first responders must be clearly identifiable to those responsible for the decision to grant access and those working at the facility,
    b. A means of access may be provided to the senior first responder (such as the chief of the fire department) to allow for access but such means of entry must be kept protected against unauthorized access or use (such as through a sealed key system), and
    c. Where the means of access may be provided under controlled conditions, the means of disabling or disarming alarms used to detect entry shall not be provided.
    d. Control of access is intrinsically linked to the concept of zoning. Zoning involves organizing a facility into distinct areas in order to control access by the public and, to a lesser extent, by personnel. The first step in this process is ensuring that the appropriate zoning requirements are identified. The definitions and requirements for public, reception, operations, security and high security zones are drawn directly from the Operational Standard for Physical Security (Section 6.2 – Hierarchy of Zones).





## Access to Personnel

16. Access controls associated with protecting persons must take into account the general conditions above in addition to the following specific conditions:
    a. Protection of persons against reasonably predictable threats as assessed through the threat and risk assessment process (such as for employees, etc.),
    b. The right to have access to government services as long as not posing a threat to personnel, and
    c. The need to protect persons, even if not directly involved in the situation except through their presence, against preventable or avoidable harm (such as the public).

## Access to Assets

17. Access controls associated with the protection of assets must take into account the general conditions above in addition to the following:
    a. Any special handling requirements of the asset (such as evidence handling, regulatory requirements, etc.),
    b. Any special control that may be required in order to ensure that the asset itself does not pose a hazard to persons or operations (such as described through programs such as the Workplace Hazardous Materials Information System – WHMIS);
    c. In certain circumstances, the ability to design the asset itself in such a way that the source of the sensitivity is protected but without having to restrict other levels of access unnecessarily;
    d. Any special controls needed to maintain controls over the accessibility of assets (against issues such as inappropriate or unauthorized use), the integrity of asset control systems (to prevent losses of control or losses of confidence in the overall system), or losses of availability of the asset.

## Access to Facilities or Spaces

18. Access controls associated with the protection of spaces must take into account the above in addition to the following specific requirements:
    a. Access control responsibilities shift during the construction process.
        i. Ownership remains with the general contractor until the building has reached the point of substantial completion. The Agency influences the security controls prior to the substantial completion of the facility (as indicated by the sign off process and contracting clauses).
        ii. The Agency takes primary control over access control measures for those areas where occupancy permits have been issued (after the point of substantial completion has been reached).
        iii. The Agency maintains control over access until the period at which the facility is no longer involved in supporting operations or holding sensitive assets,
    b. Those involved in the maintenance of base building services or other support services must satisfy CBSA requirements for access before being given access. It is recommended that







those providing the services identify alternates who may be asked to provide those services in periods of absence so as to avoid unnecessary disruptions or loss of availability of those services,

c. Where services are proposed that involve access to CBSA spaces, any contracting or other similar requirements must be made in consultation with the CBSA DSO or the DSO's identified delegate before the security requirements associated with the contract are considered appropriately addressed. This may involve any one or more of the following:
   i. The DSO (or delegate) must act as the security sign off for the contract,
   ii. The DSO (or delegate) must concur with the security requirements of the contract before it is put to tender or before the call up process begins, or
   iii. The DSO (or delegate) may require that CBSA assets be clearly and separately protected from access by the contractor through any combination of one or more of administrative, physical, procedural or technical security controls.

19. When authorizing access to spaces, operational routines must be considered. This includes, but is not necessarily limited to, the following:
   a. Peak periods of operations which may afford increased surveillance (detection) but which may require less interference from outside of the routine operations,
   b. Operations which may change the risks to persons, assets (including information) or operations, or
   c. Periods of reduced operations or occupancy by CBSA personnel where assets may be subject to less surveillance or the ability to respond to suspicious, unauthorized or inappropriate activity.

### Access Considerations for Operations

20. When authorizing access to Operations, the following must be taken into account:
   a. Access must be clearly based on the "need to know" and any operational security requirements. This is not to be interpreted as waiving the security screening requirements,
   b. Those Officer responsible for the operations (the senior officer present) may restrict access further than the routine where it is determined that there is an unacceptable risk to personnel, operations or the public and where such actions do not interfere with the legitimate Agency oversight mechanisms, and
   c. Those responsible for operations may, in consultation with the DSO or delegate, authorize an individual to have access in specific, finite situations and as the result of unpredictable circumstances where such access is necessary to assure the success of the operations or for the protection of persons. *It should be clear that this pertains only to emergency situations and not to routine or administrative processes.*

## Technological Considerations in Design

21. The following section pertains to technological restrictions and measures to be taken with respect to the control of access. All technical aspects are to reflect the requirements that stem from an assessment of risk pertinent to the specific location involved.







22. The specific method of access control must take into account the following:
    a. The level of protection to be afforded,
    b. The climate involved, and
    c. The operational needs at the facility.
23. When considering the technical requirements and design of locks, lead agency guidance shall be considered and, in the absence of such guidance, the requirements defined in the industry standards listed in Appendix A.

## Key Access (including other Tokens)

24. Key access may be suitable for remote facilities or facilities where the access is limited to a limited number of persons and where the use of combinations or computerized access control systems (such as through card readers) is not feasible from a cost-benefit perspective. In designing the key system, the following baselines are to be adhered to:
    a. Keys may only be issued to individuals in accordance with the general requirements identified above (need to know, security screening),
    b. Keys must be made using restricted keyways so as to prevent duplication,
    c. Keys must be serialized with a code linked to the name of the individual. Both the name of the individual and the code must be clearly recorded on issuance logs, and
    d. Master key code has to be kept by locksmith/company specialized in performing the work and the locksmith /company employees have to be cleared with the appropriate level of security;
    e. Only locking technology approved by CBSA Physical Security section is to be used. Generally, this approval will be based on any existing lead agency guidance and, where such guidance is not readily available, Underwriters Laboratory (UL) 437.
    f. *All keys are subject to control requirements so that all keys are accountable at all times and only held by those to whom access has been granted through approved means. A condition of being issued the key is the understanding that it must be surrendered to management or security immediately upon demand and not shared. When considering key control systems, the archived RCMP guidance is considered to be acceptable with respect to general controls.*

## Combination Access

25. Combination access may be suitable in circumstances where electronic access control systems are not feasible from a cost and benefit perspective but where a key access system is not feasible due to operational or other requirements.
    a. Combinations may only be issued to individuals in accordance with the general requirements identified above (need to know, security screening),
    b. Combinations are to be of adequate complexity to reduce the ability to guess combinations. This includes not using predictable sequences (such as 1111, 1234, etc.),
    c. Combinations must be changed on an annual basis. In addition, combinations including shared combinations such as safes must be changed when an employee moves to another position,







d. Where keypads or similar forms of technology is to be used, the maintenance of the equipment is to include periodic and routine cleaning in such a way as to reduce risks associated with being able to identify patterns or more frequently used keys,
e. A list of persons maintaining or holding combinations must be consistently maintained at all times, and
f. Only locking technology approved by CBSA Physical Security section is to be used. Generally, this approval will be based on any existing lead agency guidance and, where such guidance is not readily available, Underwriters Laboratory (UL) 768.

## Electronic Access Controls

26. Electronic access control systems may be suitable in circumstances where key or combination controls would become unmanageably complex or uncontrollable. In these cases, the following must be adhered to:
    a. The access control network is to maintain a clear, attestable and auditable separation with any other network in such a way that the following can be clearly demonstrated:
        i. Only those that have authority to manipulate the access control network have access to the application or system in such a way that changes to permissions, conditions, status or logs, and
        ii. Any person who has enhanced access to the other network can be clearly demonstrated as not having access to the access control network. This requirement must also be clearly auditable and take into account those that may attempt to gain inappropriate or unauthorized access to the network.
    b. The access control system, as of 01 June 2014, is to take into account interoperability at a local, regional and national level. This includes taking into account the following:
        i. The ability to add the local network to a wider area network, and
        ii. The ability to integrate other technology to the access control system, such as surveillance cameras, alarms or other measures.
    c. The Access Card (or ID) must meet national requirements (as communicated by Physical Security),
    d. Building access cards (after hours through the outside perimeter) provided by the landlord and those providing access to CBSA controlled spaces must be kept separate and should be carried separately in order to prevent a single event allowing access through both controls,
    e. Access control systems must be administered from within the area being protected and must be able to demonstrate that such protection is consistent across the network.
    f. The maintenance of such systems is to be coordinated through security and ensuring that any maintenance is done by appropriately qualified and security screened entities,
    g. Access control systems must include measures to ensure their continued availability and ability to recover from system failures.
    h. Only locking technology approved by CBSA shall be used. In cases where electronic access controls are the main level, a backup locking system for the outside perimeter controls and







for access into high security areas is to be maintained on separately keyed systems (back up locks requiring different keys based on the need to know).

### Use of Guard Forces for Access Control

27. Where guard forces are being proposed for access control purposes, the following applies:
    a. The use of guards must be clearly indicated,
    b. Their authority to require individuals to present identification and provide the requirement to be given access clearly communicated,
    c. The guards must be clearly identifiable through uniform or similar measure,
    d. The responsibilities and expectations are to be clearly defined and documented in post orders or their equivalent, and
    e. The guards must have a requirement to report to the senior officer at the site.

## Specific Access Control Measures for the Storage of Certain Assets or Materiel

### Firearms and Ammunition

28. Where controls are being emplaced around firearms and ammunition, the requirements associated with the Canadian Firearms Regulations must be taken into account as well as the results of any risk assessment pertinent to the site. Risks must be managed so as to ensure that no individual risk element is higher than the MEDIUM level.
29. Access controls are also to take into account the requirements associated with the safe handling, control, movement of firearms, and removal of the firearm from service.

### Negotiable Items

30. Where the controls are being emplaced to protect cash or negotiable items, the guidance provided for storage provided by the RCMP shall be used taking into account the following factors:
    a. The zone in which the container will be found,
    b. The value of the items being protected, and
    c. The time reasonably foreseen for a response to arrive at the site.
    d. In cases where the response time exceeds 60 minutes, a procedure must be put in place to remove negotiable items from that location and into a more controlled space in consultation with Security and Operations.
31. Controls over access to negotiable items are also to take into account accounting controls and other Comptrollership controls associated with the handling, movement, and control over negotiable items.
32. Negotiable items and classified material should not be held in the same cabinet.

### Narcotics and Precursors

33. The controls emplaced around narcotics and precursors shall adhere to the storage and access requirements associated with regulations published by Health Canada and taking into account any requirements associated with the Rules of Evidence.





34. Access controls associated with narcotics and precursors shall include a two-person integrity process or equivalent.
35. While CBSA has received an exemption from Health Canada, this is interpreted as being associated with the disposal of certain materials and does not absolve the Agency from its requirements under appropriate storage requirements.

### Explosives

36. Access to explosives shall comply with the requirements communicated under the *Explosives Act* and its applicable regulations.
37. Access controls associated with explosives shall include a two-person or equivalent integrity rule with respect to the storage and removal of explosives.
38. Explosives shall be removed for disposal by competent and trustworthy authorities at the earliest opportunity.

### Alcohol

39. Access controls associated with the mass storage of alcohol is to ensure that there is a clear accounting for all stored material. This includes a two person integrity or equivalent control.
40. Access controls associated with the mass storage of alcohol shall also take into account the potential risks associated with fire or similar factors.

### Items Posing Potential Biologic Threats

41. Access controls associated with items posing potential biologic hazards shall include measures necessary to control the release of any such threat into the environment. Such controls are to be designed in consultation with appropriate competent scientific and regulatory authority.
42. Access controls associated with biologic threats will pay particular attention to logs associated with those that have had access to those controlled spaces so as to be able to facilitate any activities undertaken to control the spread of such threats.

### Controlled Assets

43. Access control measures shall take into account the specific controlled asset and any requirements identified in an assessment of risk.
44. Where inappropriate access to a controlled asset is involved, both the failure of control and the attempt to gain access may be subject to further inquiry or investigation.
45. Where there is a loss of control over a controlled asset, the loss of control must be reported to security within 24 hours of discovery.

### Officer Notebooks

46. Officer notebooks remain the property of the Crown and Agency at all times. They must be surrendered to the Agency upon departure from the Agency and are to be stored for a period aligned with the statute of limitations associated with potential charges associated with any investigation.
47. Officer notebooks are to be handled in accordance with the Rules of Evidence.



48. Where an Officer's notebook is required and the Officer is not present, all reasonable attempts must be made (and the attempts recorded) to contact the Officer before access is given. At least three tries are to be made and allowing for suitable time for the Officer to respond.
49. Where an Officer's notebook is required by the Crown and the Officer cannot be reached to ensure that only and all responsive information is provided to the Crown, then the Officer`s Manager will review the notebook`s contents in consultation and ideally in the presence of a representative of the Agency`s legal team, to ensure that only appropriate information is provided.
50. No third party information (witness information, other officer information, etc.) except through legal processes coordinated by the Crown Attorney`s Office or the Court. Any such sensitivities or concerns are to be clearly identified before the information is provided.

### Information or Regulated Assets

51. Where controls for access are being put in place for information or assets protected under legislation or regulation where the security screening requirements do not directly address the risks associated with unauthorized or inappropriate disclosure, access control requirements will include the use of non-disclosure agreements or similar legally binding mechanisms.

## Roles and Responsibilities

52. The authority to grant access resides with the following:
    a. The manager delegated authority over the assets (in the context of including personnel, assets, information and operations and taking into account the need to manage in accordance with any outside requirements), and
    b. The Departmental Security Officer (DSO) or immediate delegate in the context of any security risk management decisions that affect the level of access.
53. The decision to grant access involves a security screening. Consequently, when adverse information is identified the file should be referred to the Personnel Security Screening Section so they can review and provide a recommendation to the DSO who will make the final decision as to the granting or denial to access our assets.
54. The Manager, Physical Security, provides or coordinates the functional guidance to the Agency with respect to all measures associated with access control for security or asset protection functions.
55. Managers are accountable and responsible for ensuring that they grant access to sensitive assets within their areas of responsibility only where the requirements defined in this standard have been met.
56. Each employee is accountable and responsible for ensuring that sensitive assets entrusted to him or her are protected in accordance with CBSA policies, standards and other forms of direction or instruction.

## Enquiries

57. Enquiries are to be forwarded to the Security and Professional Standards Directorate



## Appendix A – List of Industry Standards Used for Evaluation

Where the RCMP guidance is absent or is found to be dated, the following standards may be used to provide guidance with respect to the design for access control measures.

The following standards pertain to designs applicable in North America:

Underwriters Laboratories (UL)

- UL 72 (Tests for fire resistance of record protection equipment)
- UL 140 (Relocking devices for safes and vaults)
- UL 294 (Access control system units)
- UL 365 (Police station alarm units)
- UL 437 (Key locks)
- UL 608 (Burglar-resistant vault doors)
- UL 609 (Local burglar alarm units and systems)
- UL 636 (Holdup alarm units)
- UL 639 (Intrusion detection units)
- UL 687 (Burglar-resistant safes)
- UL 768 (Combination locks)
- UL 786 (Key locking systems)
- UL 887 (Time locking mechanism)
- UL 1023 (Household burglar alarm units)
- UL 1034 (Burglary-resistant electronic locking mechanisms)
- UL 1037 (Anti-theft alarms and devices)
- UL 1076 (Proprietary alarm units)
- UL 1610 (Central station alarm units)
- UL 2058 (High security electronic locks)

Builders Hardware Manufacturers Association/American National Standards Institute (BHMA/ANSI)

- 156.2 (Bored and preassembled locks and latches)
- 156.3 (Exit devices)
- 156.5 (Auxiliary locks)
- 156.12 (Interconnected locks and latches)
- 156.13 (Mortise locks)
- 156.18 (Materials and finishes)
- 156.23 (Electromagnetic locks)
- 156.24 (Delayed egress locks)
- 156.25 (Electrified locking devices)
- 156.29 (Exit locks and alarms)



- 156.30 (High-security locks)
- 156.31 (Electric strikes)
- 156.50 (Conventional auxiliary locks and cylinders)
- 156.68 (Recommended practices for master keying systems)

When considering locking equipment in Europe and not in the context of a Canadian Mission, the following standards apply:

European Committee for Standardization (CEN)

- EN 1047-2:2009 (Data rooms and data containers)
- EN 1143-1:2005+A1:2009 (Safes, ATM safes, strong room doors and strong rooms)
- EN 1143-2:2001 (Deposit systems)
- EN 1300:2004 (High security locks)
- EN 12209:2003 (Locks and latches, mechanically operated locks, latches and locking plates)
- EN 14450:2005 (Secure safe cabinets)

British Standards Institution (BSI)

- BS 3621:2004 (Thief resistant lock assemblies-Key egress)
- BS 7950:1997 (Casement and tilt/turn windows for domestic applications)
- BS 8220:2004 (Guide for security of buildings against crime)
- BS 8621:2004 (Thief resistant lock assemblies - Keyless egress)
- BS EN 1300:2004 (High security locks)
- BS EN 1303:2005 (Cylinders for locks)
- BS EN 1906:2002 (Lever handles and knobs)
- BS EN 1935:2002 (Single-axis hinges)
- BS EN 12320:2001(Padlocks and padlock fittings)

Other accredited testing standards may be used where they can demonstrate that the specific guidance can be shown to address the risks involved.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme pour le contrôle de l'accès

PROTECTION • SERVICE • INTÉGRITÉ

Canada

# Table des matières



Cette norme entre en vigueur le 2 février 2015.

## Objet

1. La présente norme vise à fournir une orientation claire, concise et exhaustive sur les exigences en matière de contrôle de l'accès. Le présent document contient à la fois des exigences (exprimées par les verbes devoir et falloir) et des recommandations (exprimées par le verbe pouvoir).

## But

2. La norme relative au contrôle de l'accès a pour but de décrire les conditions dans lesquelles l'accès aux biens sensibles (y compris les renseignements) peut être accordé.

## Portée

3. La présente norme s'applique à toutes les situations où une personne est proposée pour avoir accès à des biens sensibles, ou se voit accorder cet accès.
   a) La définition de « biens » est celle du Secrétariat du Conseil du Trésor du Canada.
   b) L'« accès » se définit dans le contexte où la personne se voyant accorder l'accès assure la garde, l'entretien ou le contrôle des biens (même si ce n'est que durant une courte période) de telle sorte que les moyens ou les possibilités d'endommager les biens augmentent.
   c) La présente norme s'applique à toutes les personnes, peu importe leur statut d'emploi, à qui l'accès aux biens sensibles est accordé.
   d) Lorsque des salles spécialisées sont concernées, il faut lire la présente norme opérationnelle de concert avec les exigences associées à ces locaux ou milieux, y compris les blocs d'exécution*, les salles d'armement*, les locaux de communication* et les locaux sécurisés*. Ces lignes directrices*, qui s'ajoutent aux exigences communiquées dans la présente norme, s'appliquent tout particulièrement à ces milieux.
   *Nota : Ces lignes directrices, qui sont cotées « Protégé B », sont fournies au personnel de l'ASFC ayant la cote de sécurité appropriée selon LE BESOIN DE CONNAÎTRE.

## Exigences

### Gouvernance

4. Lorsque l'Agence partage ou occupe des locaux avec une autre entité, le système de contrôle de l'accès pour l'Agence doit permettre de démontrer une séparation et un contrôle totaux. Les mesures et leur surveillance/les opérations doivent être convenues et clairement consignées par écrit dans un accord d'occupation (ou mécanisme semblable), qui comprend ce qui suit :
   a) La délimitation entre les contrôles de base de l'immeuble maintenus par Travaux publics ou Services partagés Canada et ceux maintenus par l'Agence,
   b) La nature des contrôles en place pour veiller à ce que l'ASFC continue d'assurer le contrôle sur ses locaux, notamment tout changement au système, les autorisations dans le système, la maintenance du système, ou tout autre contrôle susceptible d'influer sur la capacité de donner accès aux locaux de l'ASFC, et







   c) Le mécanisme par lequel l'accord est surveillé, notamment les exigences en matière de rapports et ceux en matière de fréquence et de participation pour toute réunion associée aux opérations.

5. Une copie de cet accord doit être fournie à l'agent de sécurité du ministère (ASM) par l'entremise de l'organisation de la sécurité régionale.
6. Des registres de contrôle de l'accès doivent être tenus pour tous les systèmes. Ces registres sont assujettis aux restrictions suivantes :
   a) Les renseignements personnels (comme les images) sont fournis à des fins d'identification des personnes et de contrôle de l'accès. Ils ne doivent pas servir à d'autres fins, sauf dans les circonstances où la personne visée par les renseignements donne son consentement éclairé,
   b) Les registres de contrôle de l'accès pour les locaux habituellement occupés (comme les étages de travail) peuvent servir à des fins d'enquête autorisée, mais ne doivent pas servir à des fins de supervision ordinaire,
   c) Une liste d'accès aux locaux peut être utilisée pour comparer les listes de ceux à qui la direction a autorisé d'accorder l'accès, et de ceux qui possèdent des permissions d'accès dans les systèmes de contrôle de l'accès, et
   d) Les registres de contrôle de l'accès pour les locaux inoccupés ou les locaux d'entreposage spéciaux qui ne sont normalement pas occupés par le personnel peuvent servir de moyens de surveiller l'accès; il s'agit alors de détecter les entrées non autorisées et ne pas de surveiller le rendement des employés.

## Conditions générales pour l'octroi de l'accès

7. Pour que l'accès ordinaire ou sans escorte aux locaux contrôlés de l'ASFC lui soit accordé, la personne doit pouvoir démontrer qu'elle a ce qui suit :
   a) Un besoin d'accéder aux locaux pour accomplir des tâches liées à l'Agence ou d'autres travaux, et
   b) Une cote de sécurité valide à un niveau correspondant au niveau de sensibilité le plus élevé des biens auquel la personne peut accéder.
8. Le besoin d'accéder se fonde sur les biens précis qui doivent être mis à la disposition de la personne pour qu'elle puisse accomplir son travail. En règle générale, l'accès est limité aux locaux ou aux biens que l'employé doit pouvoir utiliser pour répondre aux attentes de l'Agence relativement à son travail.
9. Le niveau de la cote de sécurité associée à l'accès se fonde sur le niveau de sensibilité le plus élevé, et tient compte des facteurs suivants :
   a) Le bien particulier et son niveau de sensibilité,
   b) Tous les biens (y compris les renseignements) auxquels la personne peut accéder lorsque l'accès à ce bien particulier lui est accordé, et
   c) Tous les biens (y compris les locaux et les renseignements) auxquels la personne peut être exposée de façon délibérée ou accidentelle lorsqu'elle se trouve dans les locaux renfermant le bien particulier.







**Par exemple, une personne à qui l'accès à un ordinateur (réseau « PROTÉGÉ B ») est accordé dans un secteur qui traite habituellement des renseignements « SECRET » aurait besoin d'une cote de sécurité « SECRET » en raison de l'exposition potentielle à des renseignements classifiés.*

10. L'accès doit tenir compte de la propriété du bien, y compris de ce qui suit :
    a) Toute exigence légale ou réglementaire associée au bien,
    b) Toute exigence en matière de certification ou d'accréditation associée au bien,
    c) Toute entente (comme un protocole d'entente) associée au bien,
    d) Toute décision stratégique interne et
    e) Toute entente contractuelle devant être maintenue.
11. Lorsque l'accès est requis sur une base temporaire (non habituelle), la personne proposée pour avoir accès aux biens doit être *escortée* afin que cet accès temporaire puisse lui être accordé. L'accès temporaire doit tenir compte de ce qui suit :
    a) Le besoin de se voir accorder l'accès doit pouvoir être clairement démontré et doit se fonder sur du travail autorisé par l'Agence,
    b) La personne agissant à titre d'escorte doit le faire au nom de l'Agence, elle doit posséder la capacité de détecter des actes non autorisés ou inappropriés, et elle doit s'être engagée à veiller à ce qu'une mesure appropriée soit déclenchée ou prise si une telle activité est détectée.
    c) L'escorte doit être en mesure d'attester que la personne escortée l'a été sous supervision constante.
12. Les personnes qui se voient délivrer un jeton (comme un insigne d'accès) doivent porter cet insigne de façon visible en tout temps lorsqu'elles se trouvent dans les locaux contrôlés, sauf dans les situations suivantes :
    a) Le port de ce jeton n'est pas conforme à la conception de l'équipement de protection individuelle, et l'agent en uniforme est en mesure de présenter le jeton sur demande en tout temps lorsqu'il se trouve dans les locaux ou lorsqu'il y entre,
    b) Le port de ce jeton expose l'employé à un risque lié à la santé et à la sécurité au travail. Si une telle requête est faite, elle doit l'être par écrit et comprendre des observations formulées par le comité local de la santé et de la sécurité au travail, notamment le bien-fondé de la réclamation, et
    c) Le port de ce jeton n'apporte aucune valeur intrinsèque, étant donné que les locaux contrôlés sont occupés par un seul groupe, que des employés de l'extérieur (comme les services de soutien) ou des visiteurs n'y sont pas autorisés, et que le taux de roulement du personnel (comme les affectations ou les détachements) n'y est pas élevé. Dans ces cas, il doit y avoir un processus de gestion clairement défini et communiqué pour indiquer au personnel autorisé toute cessation de fonctions qui réduit ou élimine le besoin d'accès. Cela s'applique aux agents affectés à des navires ou à des milieux équivalents.



## Exigences générales concernant tous les contrôles de l'accès

13. Lorsque des systèmes sont utilisés pour contrôler l'accès, les exigences suivantes doivent être respectées :
    a) Le système doit être configuré ou géré de telle sorte que le contrôle primaire sur les locaux de l'ASFC est exercé par l'Agence,
    b) Le système doit être configuré ou géré de telle sorte que les services de soutien n'ont pas l'occasion de donner accès, de manipuler les niveaux d'accès accordés ou de modifier les registres associés aux niveaux d'accès accordés (notamment à qui l'accès est accordé),
    c) Le système doit être configuré de telle sorte que l'accès est maintenu et contrôlé à un niveau individuel (notamment par l'utilisation d'une carte magnétique délivrée à la personne),
    d) Le principe des « serrures et clés » s'applique au niveau de protection à accorder pour le système de contrôle de l'accès. Le niveau de protection à accorder pour le système de contrôle de l'accès dépend du niveau de sensibilité le plus élevé du bien protégé.
14. Dans la conception des mesures de contrôle de l'accès, les critères de conception suivants doivent être mis en œuvre et maintenus :
    a) Des contrôles ***préventifs*** qui permettent de veiller à ce que tous ceux cherchant à avoir accès aux biens doivent recourir aux moyens (y compris l'approbation de sécurité) autorisés par l'Agence pour se voir accorder l'accès approprié,
    b) Des méthodes de ***détection*** qui comprennent la capacité de détecter les tentatives de contourner les contrôles ci-dessus de manière physique (notamment en franchissant le périmètre) ou administrative (en faisant de fausses réclamations sur la demande relative au contrôle de l'accès),
    c) Une ***intervention*** efficace ayant recours à des employés de l'Agence (s'il y a lieu) ou à des services externes retenus à cette fin, et répondant aux exigences en matière de sécurité pour se voir accorder l'accès, et
    d) Un plan, examiné et mis à l'essai sur une base périodique, pour gérer des situations prévisibles où il est déterminé que le système de contrôle de l'accès a échoué, ou il est raisonnable de croire qu'il a échoué, et pour rétablir la confiance dans le système (***reprise***).
15. Lorsque les locaux occupés sont partagés, et que l'accès doit être accordé aux premiers intervenants ou au personnel d'urgence, les mesures suivantes doivent être prises :
    a) Les premiers intervenants doivent pouvoir être clairement identifiés par ceux responsables de prendre la décision de leur donner accès, et par ceux travaillant dans l'installation,
    b) Un moyen d'accès peut être fourni au premier intervenant principal (comme le chef du service d'incendie) pour lui donner accès, mais ce moyen d'entrée doit toujours être protégé contre tout accès ou utilisation non autorisé (notamment au moyen d'un système de clé sous pli scellé), et
    c) Lorsque le moyen d'accès peut être fourni dans des conditions contrôlées, le moyen d'activation et de désactivation du système d'alarme servant à détecter les entrées n'est pas fourni.







d) Le contrôle de l'accès est intrinsèquement lié au concept du zonage. Le zonage consiste à organiser une installation en secteurs distincts afin de contrôler l'accès du public et, dans une moindre mesure, celui du personnel. La première étape de ce processus est de s'assurer que les exigences appropriées en matière de zonage sont déterminées. Les définitions et les exigences pour les zones publiques et de réception et les zones opérationnelles, de sécurité et de haute sécurité sont tirées directement de la Norme opérationnelle pour la sécurité matérielle (section 6.2 – Hiérarchie des zones).

### Accès au personnel

16. Les contrôles de l'accès associés à la protection des personnes doivent tenir compte des conditions générales ci-dessus, en plus des conditions précises qui suivent :
    a) La protection des personnes contre les menaces pouvant être raisonnablement prévues selon le processus d'évaluation des menaces et des risques (notamment pour les employés),
    b) Le droit d'avoir accès aux services gouvernementaux dans la mesure où une menace n'est pas présentée pour le personnel, et
    c) Le besoin de protéger les personnes, même si elles ne sont pas directement concernées par la situation, sauf de par leur présence, contre tout préjudice pouvant être prévenu ou évité (p. ex. le public).

### Accès aux biens

17. Les contrôles de l'accès associés à la protection des biens doivent tenir compte des conditions générales ci-dessus, en plus de ce qui suit :
    a) Toute exigence spéciale relative à la manipulation du bien (comme la manipulation de la preuve, les exigences réglementaires),
    b) Tout contrôle spécial pouvant être nécessaire pour veiller à ce que le bien même ne présente pas un danger pour les personnes ou les opérations (tel qu'il est décrit au moyen de programmes, comme le Système d'information sur les matières dangereuses utilisées au travail – SIMDUT),
    c) Dans certaines circonstances, la capacité de concevoir le bien même de telle sorte que la source de la sensibilité est protégée sans avoir à restreindre inutilement d'autres niveaux d'accès;
    d) Tout contrôle spécial nécessaire pour maintenir les contrôles sur l'accessibilité des biens (afin de protéger ceux-ci contre l'utilisation inappropriée ou non autorisée, entre autres) ou l'intégrité des systèmes de contrôle des biens (afin de prévenir la perte de contrôle ou la perte de confiance dans le système global, ou la perte de disponibilité des biens).

### Accès aux installations ou aux locaux

18. Les contrôles de l'accès associés à la protection des locaux doivent tenir compte de ce qui précède, en plus des exigences précises qui suivent :
    a) Les responsabilités à l'égard du contrôle de l'accès changent lors du processus de construction.







i) La propriété reste entre les mains de l'entrepreneur général jusqu'à ce que l'immeuble ait atteint le point d'achèvement substantiel. L'Agence influe sur les contrôles de sécurité avant que l'installation n'ait atteint le point d'achèvement substantiel (tel qu'il est indiqué selon le processus de signature et les clauses contractuelles).
ii) L'Agence assume le contrôle primaire sur les mesures de contrôle de l'accès dans les secteurs pour lesquels des permis d'occupation ont été délivrés (une fois le point d'achèvement substantiel atteint).
iii) L'Agence maintient le contrôle de l'accès jusqu'à ce que l'installation ne serve plus à des opérations de soutien ou à l'entreposage de biens sensibles,

b) Les personnes participant au maintien des services de base de l'immeuble ou d'autres services de soutien doivent répondre aux exigences en matière d'accès de l'ASFC avant que l'accès ne puisse leur être accordé. Il est recommandé que les personnes fournissant les services désignent des remplaçants pouvant être appelés à fournir ces services en leur absence afin d'éviter les perturbations inutiles ou les pertes de disponibilité des services,

c) Lorsque des services proposés nécessitent l'accès à des locaux de l'ASFC, toute exigence contractuelle ou autre exigence semblable doit être défini en consultation avec l'ASM de l'ASFC ou le délégué désigné de l'ASM avant qu'il ne puisse être considéré qu'il a été répondu de façon appropriée aux exigences en matière de sécurité associées au contrat. Les mesures suivantes peuvent être nécessaires :
i) L'ASM (ou son délégué) agit à titre de signataire du contrat pour les questions de sécurité,
ii) L'ASM (ou son délégué) approuve les exigences en matière de sécurité du contrat avant le lancement de l'appel d'offres ou le début du processus de passation de commande subséquente, ou
iii) L'ASM (ou son délégué) exige que les biens de l'ASFC soient clairement et séparément protégés contre tout accès par l'entrepreneur au moyen d'un ou de plusieurs contrôles de sécurité administratifs, matériels, procéduraux ou techniques.

19. Lorsque l'accès à des locaux est autorisé, il faut tenir compte des opérations ordinaires, notamment de ce qui suit :
a) Les périodes de pointe pouvant permettre une surveillance (détection) accrue, mais nécessiter une intervention réduite en dehors des opérations ordinaires,
b) Les opérations susceptibles d'influer sur les risques pour les personnes, les biens (y compris les renseignements) ou les opérations mêmes, ou
c) Les périodes d'opérations ou d'occupation réduites par le personnel de l'ASFC, durant lesquelles les biens pourraient être moins surveillées, ou la capacité d'intervenir en cas d'activités suspectes, non autorisées ou inappropriées pourrait être réduite.

## Considérations relatives à l'accès aux opérations

20. Lorsque l'accès aux opérations est autorisé, il faut tenir compte de ce qui suit :







a) L'accès doit clairement se fonder sur le « besoin deconnaître» et sur toute exigence opérationnelle en matière de sécurité, ce ne doit pas être interprété comme une renonciation aux exigences de contrôle de sécurité, ,
b) L'agent responsable des opérations (l'agent supérieur sur les lieux) peut restreindre l'accès davantage que ne le prévoient les processus habituels, lorsqu'il est déterminé qu'il existe un risque inacceptable pour le personnel, les opérations ou le public, et que ces mesures ne portent pas atteinte aux mécanismes de surveillance légitimes de l'Agence, et
c) Le responsable des opérations peut, en consultation avec l'ASM ou son délégué, donner accès à une personne dans des situations précises limitées, et en raison de circonstances imprévisibles, où cet accès est nécessaire pour assurer la réussite des opérations ou la protection des personnes. *Il doit être clair que cette exception ne s'applique qu'aux situations d'urgence et non pas aux processus habituels ou administratifs.*

## Considérations technologiques relatives à la conception

21. La section suivante porte sur les restrictions technologiques et les mesures à prendre en ce qui concerne le contrôle de l'accès. Tous les aspects techniques doivent tenir compte des exigences découlant d'une évaluation des risques pour l'emplacement précis visé.
22. La méthode précise de contrôle de l'accès doit tenir compte de ce qui suit :
    a) Le niveau de protection requis,
    b) Le climat et
    c) Les besoins opérationnels de l'installation.
23. Au moment de tenir compte des exigences techniques et de la conception des serrures, il faut suivre l'orientation de l'organisme responsable et, en l'absence d'une telle orientation, les exigences définies selon les normes de l'industrie qui sont énumérées à l'annexe A.

### Accès par clé (y compris d'autres jetons)

24. L'accès par clé peut convenir à des installations éloignées ou à des installations auxquelles l'accès est limité à un nombre restreint de personnes, et où l'utilisation de numéros de combinaison ou de systèmes informatisés de contrôle de l'accès (tels que des lecteurs de carte) n'est pas réalisable sur le plan des coûts-avantages. La conception du système de clé doit respecter les principes de base suivants :
    a) Les clés ne peuvent être délivrées à des personnes que selon les exigences générales énoncées précédemment (besoin deconnaître, contrôle de sécurité),
    b) Les clés doivent être fabriquées au moyen d'entrées de clé restreintes afin de prévenir la duplication,
    c) Les clés doivent être sérialisés avec un code lié au nom de l'individu. Tant le nom de la personne et le code et la clé émis doit être clairement consignés dans le registre des clés délivrés, et
    d) Le code de passe-partout doit être gardé par le serrurier/l'entreprise spécialisée ayant fait l'objet d'un contrôle de sécurité au niveau approprié;



e) Seule la technologie de verrouillage approuvée par la Section de la sécurité matérielle de l'ASFC doit être utilisée. En règle générale, cette approbation se fonde sur l'orientation existante de l'organisme responsable et, en l'absence d'une telle orientation, sur la norme 437 des Laboratoires des assureurs (UL).

f) *Toutes les clés sont assujetties aux exigences en matière de contrôle, ce qui signifie qu'elles doivent pouvoir être repérées en tout temps, et qu'elles ne sont détenues que par des personnes à qui l'accès a été accordé par les moyens approuvés. Une condition liée à la délivrance de la clé est la compréhension que celle-ci doit être restituée à la direction ou à la Sécurité dès que la demande en est faite, et qu'elle ne doit pas être partagée. Les systèmes de contrôle de clé doivent être conformes à l'orientation archivée de la Gendarmerie royale du Canada (GRC), qui est considérée comme étant acceptable en ce qui concerne les contrôles généraux.*

## Accès à combinaison

25. L'accès à combinaison peut convenir dans des circonstances où des systèmes électroniques de contrôle de l'accès ne sont pas réalisables sur le plan des coûts-avantages, et où un système d'accès par clé n'est pas possible en raison d'exigences opérationnelles ou autres.

    a) Les numéros de combinaison ne sont délivrés à des personnes que selon les exigences générales énumérées précédemment (besoin de connaître, contrôle de sécurité),

    b) Les numéros de combinaison doivent être suffisamment complexes pour réduire le risque qu'on les devine. Entre autres, il ne faut pas utiliser des séquences prévisibles (comme 1111, 1234, etc.),

    c) Les numéros de combinaison doivent être changés sur une base annuelle. En outre, les numéros de combinaison partagés, notamment pour les coffres-forts, doivent être changés lorsqu'un employé est muté dans un autre poste,

    d) Lorsque des claviers numériques ou des formes de technologie semblables sont utilisés, l'entretien de l'équipement doit comprendre le nettoyage périodique et de routine afin de réduire le risque qu'on puisse détecter des tendances ou des clés utilisées plus fréquemment,

    e) Une liste des personnes maintenant ou détenant un numéro de combinaison doit être tenue à jour en tout temps et de façon uniforme, et

    f) Seule la technologie de verrouillage approuvée par la Section de la sécurité matérielle de l'ASFC doit être utilisée. En règle générale, cette approbation se fonde sur l'orientation existante de l'organisme responsable et, en l'absence d'une telle orientation, sur la norme 768 des Laboratoires des assureurs (UL).

## Contrôles de l'accès électroniques

26. Les systèmes électroniques de contrôle de l'accès peuvent convenir dans des circonstances où le contrôle par clé ou à combinaison serait trop complexe et ne pourrait pas être géré ou surveillé. Dans ces cas, il faut respecter les principes suivants :



a) Le réseau de contrôle de l'accès doit maintenir une séparation claire pouvant être attestée et vérifiée avec tout autre réseau de telle sorte que le respect des exigences suivantes peut être démontré :
   i) Seules les personnes autorisées à manipuler le réseau de contrôle de l'accès ont accès à l'application ou au système afin de changer les permissions, les conditions, le statut ou le registre, et
   ii) Il doit pouvoir être clairement démontré que la personne ayant un accès avancé à l'autre réseau n'a pas accès au réseau de contrôle de l'accès. Le respect de cette exigence doit aussi pouvoir être clairement vérifié, et il faut tenir compte du fait que des personnes pourraient tenter d'accéder au réseau de façon inappropriée ou non autorisée.
b) Le système de contrôle de l'accès, à compter du 1er juin 2014, doit tenir compte de l'interopérabilité à l'échelle locale, régionale et nationale, notamment de ce qui suit :
   i) La capacité d'ajouter le réseau local à un réseau local élargi, et
   ii) La capacité d'intégrer d'autres technologies au système de contrôle de l'accès, comme des caméras de surveillance, des alarmes ou d'autres dispositifs.
c) L'insigne d'accès (ou la carte d'identité) doit répondre aux exigences nationales (telles qu'elles ont été communiquées par la Sécurité matérielle),
d) Les cartes d'accès à l'immeuble (après les heures, par le périmètre extérieur) qui sont fournies par le propriétaire, et celles qui donnent accès aux locaux contrôlés de l'ASFC, doivent être gardées et portées séparément afin d'empêcher qu'un événement unique confère un accès par les deux systèmes de contrôle,
e) Les systèmes de contrôle de l'accès doivent être administrés depuis l'intérieur de la zone protégée, et il faut pouvoir démontrer que cette protection est uniforme à l'échelle du réseau.
f) L'entretien de ces systèmes doit être coordonné par la Sécurité, et il faut veiller à ce que tout entretien effectué le soit par des entités possédant les qualifications appropriées et ayant fait l'objet d'un contrôle de sécurité,
g) Les systèmes de contrôle de l'accès doivent comprendre des mesures visant à assurer leur disponibilité continue et leur capacité de reprise à la suite de défaillances.
h) Seule la technologie de verrouillage approuvée par l'ASFC doit être utilisée. Dans les cas où les contrôles de l'accès électroniques constituent le principal système utilisé, un système de verrouillage de remplacement pour les contrôles du périmètre extérieur et l'accès aux zones de haute sécurité doit être maintenu au moyen de systèmes de clé séparés (serrures de remplacement nécessitant des clés différentes selon le besoin de savoir).

### Utilisation de gardiens pour le contrôle de l'accès

27. Lorsque des gardiens sont proposés à des fins de contrôle de l'accès, les exigences suivantes s'appliquent :
   a) Le recours à des gardiens doit être clairement indiqué,



b) Le pouvoir de ceux-ci d'exiger aux personnes de présenter des pièces d'identité et de respecter l'exigence pour avoir accès aux locaux doit être clairement communiqué,
c) Les gardiens doivent pouvoir être clairement identifiés au moyen de leur uniforme ou de mesures semblables,
d) Les responsabilités et les attentes doivent être clairement définies et consignées par écrit dans des ordres de poste ou leur équivalent, et
e) Les gardiens doivent obligatoirement relever de l'agent principal sur les lieux.

## Mesures précises de contrôle de l'accès pour l'entreposage de certains biens ou matières

### Armes à feu et munitions

28. Lorsque des contrôles visant des armes à feu et des munitions sont mis en place, les exigences associées aux règlements relatifs aux armes à feu au Canada doivent être respectés, ainsi que des résultats de toute évaluation des risques pour l'emplacement. Il faut gérer les risques afin qu'aucun élément de risque particulier ne dépasse le niveau MODÉRÉ.
29. Les contrôles de l'accès doivent également tenir compte des exigences associées à la manipulation, au contrôle et au mouvement sécuritaires des armes à feu, ainsi qu'au retrait de service de celles-ci.

### Effets négociables

30. Lorsque des contrôles visant des espèces ou des effets négociables sont mis en place, il faut suivre l'orientation fournie par la GRC en tenant compte des facteurs suivants :
    a) La zone dans laquelle le conteneur se trouvera,
    b) La valeur des effets protégés et
    c) Le délai raisonnable prévu pour l'arrivée des intervenants sur les lieux.
    d) Lorsque le délai d'intervention dépasse 60 minutes, il faut mettre en place une procédure pour le retrait des effets négociables de cet emplacement et leur transfert vers une zone offrant un contrôle accru, en consultation avec la Sécurité et les Opérations.
31. Les contrôles de l'accès aux effets négociables doivent également tenir compte des contrôles comptables et d'autres mesures du Contrôle associées à la manipulation, au mouvement et au contrôle des effets négociables.
32. Des effets négociables et des documents classifiés ne doivent pas être gardés dans le même classeur.

### Stupéfiants et précurseurs

33. Les contrôles visant les stupéfiants et les précurseurs qui sont mis en place doivent répondre aux exigences en matière d'entreposage et d'accès qui sont associées aux règlements publiés par Santé Canada, en plus de tenir compte de toute exigence associée aux règles de la preuve.
34. Les contrôles de l'accès associés aux stupéfiants et aux précurseurs doivent comprendre un processus relatif à l'intégrité assurée par deux personnes, ou une règle équivalente.



35. Bien que l'ASFC ait obtenu une exemption de Santé Canada, cette exemption est associée à l'élimination de certaines matières, et elle ne décharge pas l'Agence des exigences appropriées en matière d'entreposage.

## Explosifs

36. L'accès aux explosifs doit être conforme aux exigences prévues par la *Loi sur les explosifs* et son règlement.
37. Les contrôles de l'accès associés aux explosifs doivent comprendre un processus relatif à l'intégrité assurée par deux personnes, ou une règle équivalente pour l'entreposage et le retrait des explosifs.
38. Les explosifs doivent être retirés à des fins d'élimination par les autorités compétentes de confiance dès que possible.

## Alcool

39. Les contrôles de l'accès associés à l'entreposage en masse d'alcool visent à s'assurer qu'il y a une comptabilisation claire de tout l'alcool entreposé. Entre autres, il faut utiliser un processus relatif à l'intégrité assurée par deux personnes, ou un contrôle semblable.
40. Les contrôles de l'accès associés à l'entreposage en masse d'alcool doivent également tenir compte des risques potentiels d'incendie ou de facteurs semblables.

## Articles présentant des menaces biologiques potentielles

41. Les contrôles de l'accès associés aux articles susceptibles de présenter des menaces biologiques potentielles comprennent les mesures nécessaires pour prévenir leur rejet dans l'environnement. Ces contrôles doivent être conçus avec les autorités réglementaires et scientifiques compétentes.
42. En particulier, les contrôles de l'accès associés aux menaces biologiques doivent comprendre des registres des personnes qui ont eu accès aux locaux contrôlés afin que toute activité de prévention de la propagation de telles menaces puisse être menée.

## Biens contrôlés

43. Les mesures de contrôle de l'accès doivent tenir compte des biens contrôlés précis et de toute exigence découlant d'une évaluation des risques.
44. En cas d'accès inapproprié aux biens contrôlés, tant la défaillance du contrôle que la tentative d'accès peuvent faire l'objet d'une enquête approfondie.
45. En cas de perte de contrôle des biens contrôlés, l'incident doit être signalé à la Sécurité dans les 24 heures suivant sa découverte.

## Carnets des agents

46. Les carnets des agents demeurent en tout temps la propriété de la Couronne et de l'Agence. Ils doivent être restitués à l'Agence au moment de quitter celle-ci, et ils doivent être conservés durant une période conforme à la loi sur la prescription associée aux accusations potentielles découlant de toute enquête menée.
47. Les carnets des agents doivent être manipulés conformément aux règles de la preuve.



48. Lorsqu'un carnet de l'agent est requis, et que l'agent en question n'est pas sur les lieux, il faut déployer tous les efforts raisonnables (et enregistrer ces efforts) pour joindre l'agent avant de donner accès à son carnet. Il doit y avoir au minimum trois tentatives de joindre l'agent, et il faut accorder à celui-ci un délai de réponse approprié.
49. Lorsqu'un carnet de l'agent est requis par la Couronne, et que l'agent en question ne peut pas être joint pour veiller à ce que seule et toute l'information pertinente soit fournie à la Couronne, le gestionnaire de l'Agence examine le contenu du carnet, en consultation avec un représentant des Services juridiques de l'Agence et, idéalement, en présence d'un tel représentant, pour veiller à ce que seule l'information pertinente soit fournie.
50. Aucun renseignement de tiers (renseignements de témoins, autres renseignements d'agents, etc.) ne doit pas être révélé sauf par des moyens légaux coordonnés par le bureau du procureur de la Couronne ou le tribunal, ne doit être fourni. Toute sensibilité ou préoccupation connexe doit être clairement déterminée avant que l'information ne soit fournie.

### Renseignements ou biens réglementés

51. Lorsque les contrôles de l'accès mis en place visent des renseignements ou des biens protégés par des lois ou des règlements, et que les exigences en matière de contrôle de sécurité ne traitent pas directement des risques liés à la communication non autorisée ou inappropriée, ces exigences doivent comprendre l'utilisation d'ententes de non-communication ou de mécanismes semblables juridiquement contraignants.

## Rôles et responsabilités

52. Le pouvoir de donner accès appartient :
    a) Au gestionnaire ayant les pouvoirs délégués pour les biens, notamment en ce qui a trait au personnel, aux biens, aux renseignements et aux opérations, et compte tenu du besoin de gérer conformément à toute exigence externe, et
    b) À l'agent de sécurité du ministère (ASM) ou à son délégué immédiat pour ce qui est de toute décision concernant la gestion des risques pour la sécurité qui influe sur le niveau d'accès.
53. La décision de donner accès nécessite une décision concernant la gestion des risques pour la sécurité. Par conséquent, lorsqu'une personne ne répond pas aux exigences minimales pour se voir accorder l'accès, la mesure doit être approuvée en consultation et avec l'accord de l'ASM ou, si celui-ci l'autorise, de son délégué.
54. Le gestionnaire, Sécurité matérielle, fournit ou coordonne l'orientation fonctionnelle à l'Agence pour toutes les mesures associées au contrôle de l'accès qui visent les fonctions de sécurité ou de protection des biens.
55. Il incombe aux gestionnaires de ne donner accès à des biens sensibles dans leur sphère de responsabilité que lorsque les exigences définies dans la présente norme sont respectées.
56. Il incombe à chaque employé d'assurer la protection des biens sensibles qui lui sont confiés conformément aux politiques, aux normes, ainsi qu'à l'orientation ou aux directives de l'ASFC.



## Demandes de renseignements

57. Les demandes de renseignements doivent être adressées à la direction de la sécurité et des normes professionnelles.

## Annexe A – Liste des normes de l'industrie à des fins d'évaluation

Lorsque l'orientation de la GRC est inexistante ou désuète, il faut respecter les normes suivantes pour fournir une orientation concernant la conception des mesures de contrôle de l'accès.

Les normes de conception suivantes s'appliquent à l'Amérique du Nord :

Laboratoires des assureurs (UL)

- UL 72 (essais de résistance au feu de l'équipement de protection des dossiers)
- UL 140 (dispositifs de reverrouillage pour les coffres-forts et les chambres fortes)
- UL 294 (unités de système de contrôle de l'accès)
- UL 365 (unités d'alarme de poste de police)
- UL 437 (serrures à clé)
- UL 608 (portes de chambre forte à l'épreuve des voleurs)
- UL 609 (unités et systèmes d'alarme antivol locaux)
- UL 636 (unités d'alarme de hold-up)
- UL 639 (unités de détection d'intrusion)
- UL 687 (coffres-forts à l'épreuve des voleurs)
- UL 768 (serrures à combinaison)
- UL 786 (systèmes de verrouillage par clé)
- UL 887 (mécanismes de verrouillage différé)
- UL 1023 (unités d'alarme antivol résidentielles)
- UL 1034 (mécanismes de verrouillage électronique à l'épreuve des voleurs)
- UL 1037 (alarmes et dispositifs antivol)
- UL 1076 (unités d'alarme exclusives)
- UL 1610 (unités d'alarme de centrale)
- UL 2058 (serrures à verrouillage électronique de haute sécurité)

Builders Hardware Manufacturers Association/American National Standards Institute (BHMA/ANSI)

- 156.2 (serrures et verrous encastrés et pré-assemblés)
- 156.3 (dispositifs d'issue)
- 156.5 (serrures auxiliaires)
- 156.12 (serrures et verrous combinés)
- 156.13 (serrures à mortaise)
- 156.18 (matériaux et finis)
- 156.23 (serrures électromagnétiques)
- 156.24 (serrures à retardement d'issue)
- 156.25 (dispositifs de verrouillage électrifiés)
- 156.29 (serrures et alarmes d'issue)



- 156.30 (serrures de haute sécurité)
- 156.31 (gâches électriques)
- 156.50 (serrures auxiliaires et barillets traditionnels)
- 156.68 (pratiques recommandées pour les systèmes de fabrication de passe-partout)

Les normes suivantes s'appliquent à l'équipement de verrouillage en Europe, sauf dans les missions canadiennes :

Comité européen de normalisation (CEN)

- EN 1047-2:2009 (salles de données et conteneurs de données)
- EN 1143-1:2005+A1:2009 (coffres-forts, coffres-forts de guichet automatique, portes de chambre forte et chambres fortes)
- EN 1143-2:2001 (systèmes de dépôt)
- EN 1300:2004 (serrures de haute sécurité)
- EN 12209:2003 (serrures et verrous, serrures à actionnement mécanique, verrous et plaques de verrouillage)
- EN 14450:2005 (armoires de sûreté)

British Standards Institution (BSI)

- BS 3621:2004 (vérins de verrouillage à l'épreuve des voleurs – issue avec clé)
- BS 7950:1997 (bâtis et fenêtres oscillo-battantes pour usage résidentiel)
- BS 8220: 2004 in English here just question mark???? (guide pour la protection des immeubles contre le crime)
- BS 8621:2004 (vérins de verrouillage à l'épreuve des voleurs – issue sans clé)
- BS EN 1300:2004 (serrures de haute sécurité)
- BS EN 1303:2005 (barillets pour serrures)
- BS EN 1906:2002 (becs-de-canes et boutons)
- BS EN 1935:2002 (charnières à un seul axe)
- BS EN 12320:2001(cadenas et ferrures)

D'autres normes d'essai accrédité peuvent être utilisées si elles permettent de démontrer que les risques en cause sont gérés en fonction de l'orientation précise.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Guidelines for Identification Cards

PROTECTION • SERVICE • INTEGRITY

Canada

Canada Border Services Agency | Agence des services frontaliers du Canada



# Table of Contents



These guidelines take effect on February 2, 2015.

**Purpose**

The Canada Border Services Agency (CBSA) security controlled assets guide describes the identification cards and building passes. It is designed to reduce the risk of unauthorized access to sensitive information and assets.

**Application**

This guide is applicable to all CBSA employees (permanent, term, casual, and part-time), contract and private agency personnel, and to individuals seconded or assigned to the CBSA (including students).

**General**

CBSA identification (ID) cards and building passes must be worn at all times while on CBSA premises so they can easily be seen, with the exceptions of uniformed border services officers or where the wearing of the ID card or pass will cause a serious safety hazard. In instances where the wearing of the ID card is not appropriate, the employee must still carry/have it in their possession.

The bearing of any specific Identification Card / Access Badge does not allow an individual the right to bypass physical security or safety access controls put in place by the officer responsible for that space. A condition of issuance is that the individual will respect the legitimate authority of the management accountable for the spaces being given access and adhere to the implemented security and safety controls.

CBSA identification cards and building passes are the property of CBSA and must be used only for the purposes for which they are issued. A card or pass may be revoked, at management's discretion or by the Director, Infrastructure and Information Security Directorate (IISD).

Except for visitor passes, no ID card or access pass will be issued to anyone who does not have a valid Security Clearance or Reliability status.

Requests for the issuance of identification cards or contractor passes must be supported by appropriate documentation such as a completed Controlled Assets Form (BSF208) signed by the manager and employee.

The loss of an identification card or a pass must be reported immediately to the issuing authority. The completion of a Security Incident Form (Form BSF152) is mandatory. A lost identification card will be re-issued after the loss has been reported to the issuing authority.

The only authorized identification cards and building pass templates are those that have been issued by the Physical Security Section, Security and Professional Standards Directorate (SPSD) to the Regional and



Headquarters Security Offices to be loaded on all identification card computer systems. These templates must not be modified.

Identification, authority and designation cards are produced using electronic master artwork files only. Overprinting of cards, including the application of an employee photo and clearance level markers, is also completed using electronic master artwork files held by Security and Professional Standards.

**Types of Identification Cards and Passes**

Identification cards are printed on the supplied pre-printed CBSA card stock while passes (Temporary, Visitor, Recruit, and Contractor) are printed on the blank/white card stock. Additional access token for room/building access in line with the Operational Standard for Access Control will be required.

**Blue Bar ID:**

The blue bar ID card is identified by a blue expiry date bar above the centered picture. The blue bar ID card is issued to indeterminate (permanent) CBSA employees. The cardholder is authorized to have access to CBSA facilities across Canada, subject to local access control procedures.

Silent hours are to be identified on the card by a red "Q" in the upper right of the printed picture on card. Clearance level of this individual is identified by a color square in the bottom right next to the picture (see Appendix A - Symbol Legend).

**Temporary Pass:**

The Temporary Pass is identified by a Blue "T" centered on the card with a blue bar identifying the employee as an indeterminate employee. To the bottom right of the "T" is the clearance level of that employee.

The Temporary Pass is designed primarily to be issued to individuals who are indeterminate employees of the CBSA who have misplaced or forgotten their identification card. The pass must not leave the facility for which it was issued and must be returned to the issuing office at the end of each visit. No escort is required.

**The Visitor Pass:**

The Visitor Pass is identified by a red V with a red expiry bar. The Visitor Pass is to be issued to individuals who are not CBSA employees and who require access to a facility or an office for a period of up to one day. Such individuals must always be escorted in and out of restricted areas by a CBSA employee who has authorized access. The pass must not leave the facility for which it was issued and must be returned to the issuing office at the end of each visit.

**Recruit Pass:**

The Recruit Pass is identified by a red "R" and a red expiry bar. This card is to be strictly used by the CBSA College – Main Campus (Rigaud, Quebec) or the incoming recruits. The card is not to be used in any other facility.



Clearance level of this individual is identified by a color square in the bottom right next to the picture (see Appendix A Symbol Legend).

## Contractor Passes:

Two contractor cards will be utilized.

1. Contracted resources/consultants

The contractor card for this type of personnel is identified by a green C and green expiry bar. This card will be utilized to identify contracted resources/consultants. The contractor card is signed out in the log but is only returned after the contract has expired. The CBSA site contact (Manager/Supervisor/Security Officer) must be clearly identified on the pass. The contractor card for contracted resources/consultants may remain in the possession of that consultant until the end of his or her term. No escort required for these contractors based on level of clearance and zone of entry.

Contractor cards are issued to each contractor and photographs are necessary on each card to identify the individual. The clearance level of the contractor is also identified to the bottom right of the green C.

2. Trade personnel

The contractor card for this type of personnel is identified by a red C and red expiry bar. The contractor must always be escorted in and out of restricted areas by a CBSA employee who has authorized access. The contractor card for contracted trade personnel is to be signed out on a daily basis for the length of the contract. The CBSA site contact must be clearly identified on the pass. The pass must not leave the facility for which it was issued and must be returned to the issuing office at the end of each visit.

**Green Bar ID pass for temporary or part-time employees:**

The Green Bar ID pass for temporary or part-time employees is identified by a green expiry date bar above the picture, **without the "C".** The green bar ID card is issued to **temporary or part-time employees** that include for example: Casual, Term, Part-time, Secondment, Assignment employees where there is an employer/employee relationship but not on a full time basis. This also includes Students, Coop Students however **not** the Recruits as defined above. The cardholder is authorized to have access to CBSA facilities across Canada, subject to local access control procedures.

Silent hours are to be identified on the card by a red "Q" to the upper right of the printed picture on card. Clearance level of this individual is identified by a color square in the bottom right next to the picture (see Appendix A - Symbol Legend).

## Designation and Authority Cards:



For more information regarding Designation and Authority cards please consult CBSA Enforcement Manual Part 8 Enforcement Forms.

## 1 Responsibilities

The issue, control, and retrieval of identification cards and building passes, must be by a CBSA Issuing Delegated Authority. Regional Security or in Headquarters the HQ Security Section is the issuing authority and can approve the delegation to individuals required to issue the cards and building passes (e.g. commissionaires).

## 2 Employee Awareness

Employees should notify their supervisor who will inform Regional or Headquarters Security when they become aware of persons without an identification card/pass, CBSA escort or wearing an expired identification card while in a CBSA operational zone.

## 3 Procedures

### 3.1 Issuance

Identification cards must only be issued to individuals who have met the CBSA Personnel Security Screening requirements. This procedure must be completed prior to individuals starting their work-related duties.

The manager or alternate will complete a Controlled Assets Form (BSF208) and forward it to Regional or Headquarters Security Office for processing.

Regional or Headquarters Security will verify that the personnel security screening requirements have been met and contact the individual for a photograph.

Once the photograph has been taken and the card has been produced the individual and the CBSA Issuing Authority will sign the Controlled Assets Form (BSF208). The completed BSF208 will be retained in Regional or Headquarters Security Office. (This can be coordinated within the districts).

The identification cards should be issued with one plastic carrying case and a lanyard. The identification cards must be produced using the preprinted card and or templates supplied by Physical Security Section (PSS). The passes are to be produced using the blank card and the template that was supplied by PSS.

The visitor/temporary pass must not leave the facility for which they were issued and must be returned to the issuing office at the end of each visit. Before issuing a pass the issuing authority shall verify the individual's identification by reviewing their Federal or Provincial government issued photo identification. All contractors presenting themselves on CBSA grounds who do not have a CBSA official contractor card are to be issued visitor cards and escorted at all times. A log control book shall be used to record the following information:

- the facility address;
- person's name;
- pass ID number;



- person's personal identification number (i.e. taken from photo ID);
- date/time of issuance;
- name of the person who issued it;
- date/time of retrieval;
- name of the person who retrieved the card; and
- CBSA site contact responsible for the visitor.

These logs must be secured in an approved cabinet along with the visitor/temporary passes when not in use. The logs shall be kept for audit purposes.

A contractor pass can only be issued when it is demonstrated that the Contractor meets the security requirements defined in the contract. When considering the level of security screening to be used, the Security Requirements Checklist (SRCL) provides the authoritative methodology.

The manager or project authority will complete a Controlled Assets Form (BSF208) and forward it to the Regional or Headquarters Office for processing. The BSF208 shall be kept by Regional or Headquarters Security.

Regional or Headquarters Security will verify that the screening requirements have been met and contact the contractor or project authority to make arrangements for a photograph.

Regional or Headquarters Security will provide the authorized contractor passes to the project authority or manager; the project authority, manager or delegate will issue a pass by verifying the individual's identification by reviewing their Federal or Provincial government issued photo identification. A log control book shall be used to record the following information:

- the facility address;
- contractor name;
- company that they work for;
- date/time of issuance;
- name of the person who issued it;
- date/time of retrieval;
- name of the person who retrieved the card; and
- CBSA site contact responsible for the visitor.

The contractor pass (red pass with "C" marking as per Appendix B) must not leave the facility for which it was issued and should be returned to the issuing office at the end of each visit. None-CBSA employees contracted to perform work on behalf of the Agency or for the Agency can be issued a contractor card (green pass with "C" marking as per appendix B) with the privilege of not having to sign in or out the log book, at the discretion of the Regional or Headquarters Security Manager. The project authority or manager will return all contractor passes (green pass with "C" marking) to Regional or Headquarters Security upon the completion of the contract or if the pass has expired.



### 3.2 Photographs

Photographs for the identification cards and passes must meet the following criteria:

- the image must be clear, sharp, centered and in focus;
- use a light blue background without shadows;
- show full front view of your head and shoulders, the face and shoulders must be centered in the photo and squared to the camera;
- eyes must be open and clearly visible and should not appear to be red;
- glasses, including tinted ones with prescription, may be worn as long as the eyes are clearly visible, sunglasses are unacceptable;
- facial expression must be neutral (not frowning or smiling) with the mouth closed;
- hats and other head coverings are not permitted except when worn for religious or medical reasons and only if the full facial features are clearly visible;
- Photographs must be stored in jpeg format, using last name, first, and year of photo, for example Doe, Jane, 2011; and
- Photographs must be re-taken every five (5) years or when major identification features have changed.

### 3.3 Returning the Identification Card

Identification cards are to be returned to the Regional or Headquarters Security Office using the Controlled Assets Form (BSF208) accompanied by an Employee Departure Form (BSF270).

Returns are necessary when one of the following conditions apply:

- the employee ceases to be an employee of the Agency;
- the card has expired;
- an individual ceases to be an employee at the location for which the identification card was issued;
- in extreme circumstances where there is an immediate threat (i.e. Workplace violence) and when requested by the management responsible for the space to which the individual has been given access or requested by a member of the Physical Security organization when acting under the authority of the Departmental Security Officer;
- The employee commences a temporary absence over four months from the position and duties entitling the identification card.

## 4 Loss or Theft

Reporting lost and stolen identification cards immediately is essential to prevent compromise or to lessen the risk of compromise. The owner of the identification card must complete a Security Incident Form (BSF152) and complete a Controlled Assets Form (BSF208) to report the loss or theft of their identification card. The BSF152 shall be signed by the employee's director and sent to Regional or Headquarters Security. A completed Controlled Assets Form (BSF208) must be attached to the BSF152 form for the issuance of a replacement identification card.



## 5 Disposal

Identification cards/passes will be destroyed by the Regional or Headquarters Security Office only. The return of the identification card/pass for destruction is essential in the control process.

## 6 Accountability Process

The administration of this guideline will be monitored through security inspections conducted by the Security and Professional Standard Directorate, Regional or Headquarters Security and through security sweeps conducted by the Regional or Headquarters Security Officers.

The Internal Audit and Program Evaluation Directorate of the Corporate Affairs Branch (CAB) will provide an independent level of assurance by performing internal audits.

## 7 Contact for Updates

Persons seeking clarification and updates with respect to this document should contact their Regional or Headquarters Security Office or the Manager, Physical Security Section, Security and Professional Standards Directorate (SPSD).

## 8 Deviation from Standard

Deviation from the standard must be approved by HQ Physical Security Section.

For further clarification, contact the SPSD Manager, Physical Security (NHQ-Ottawa) at: CBSADSOSecurity@cbsa-asfc.gc.ca

HQ Manager, Physical Security



# Appendix A

## Symbol Legend

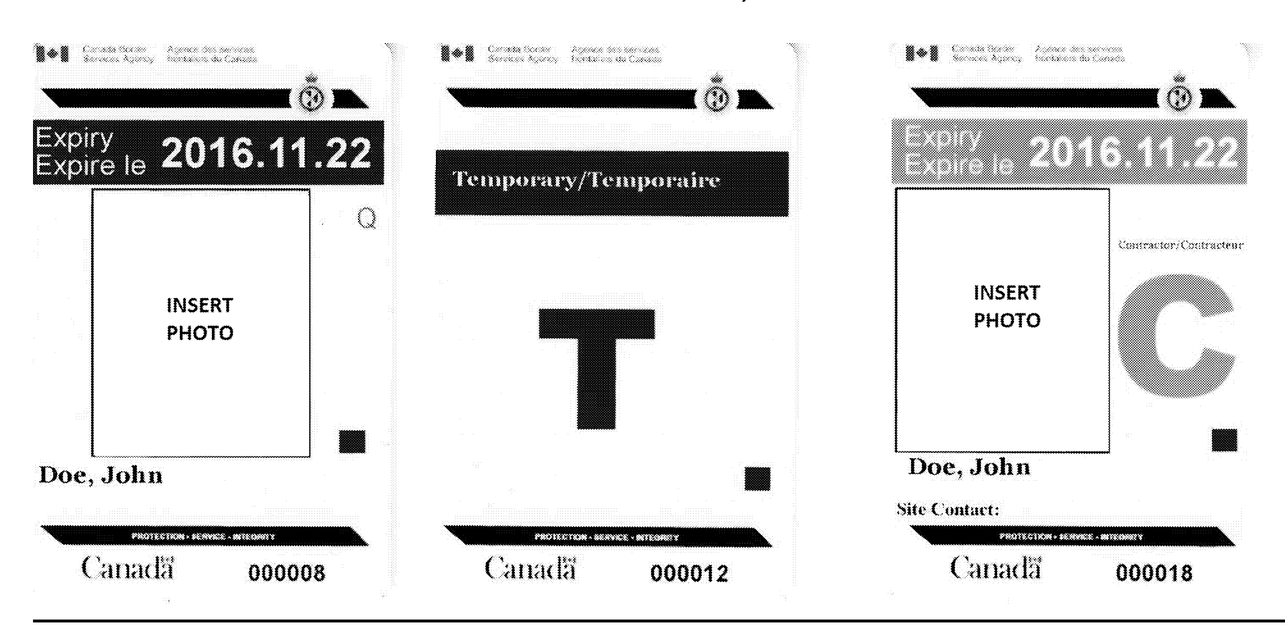
Reliability
Secret
Top Secret
Silent Hours Q



# Appendix B

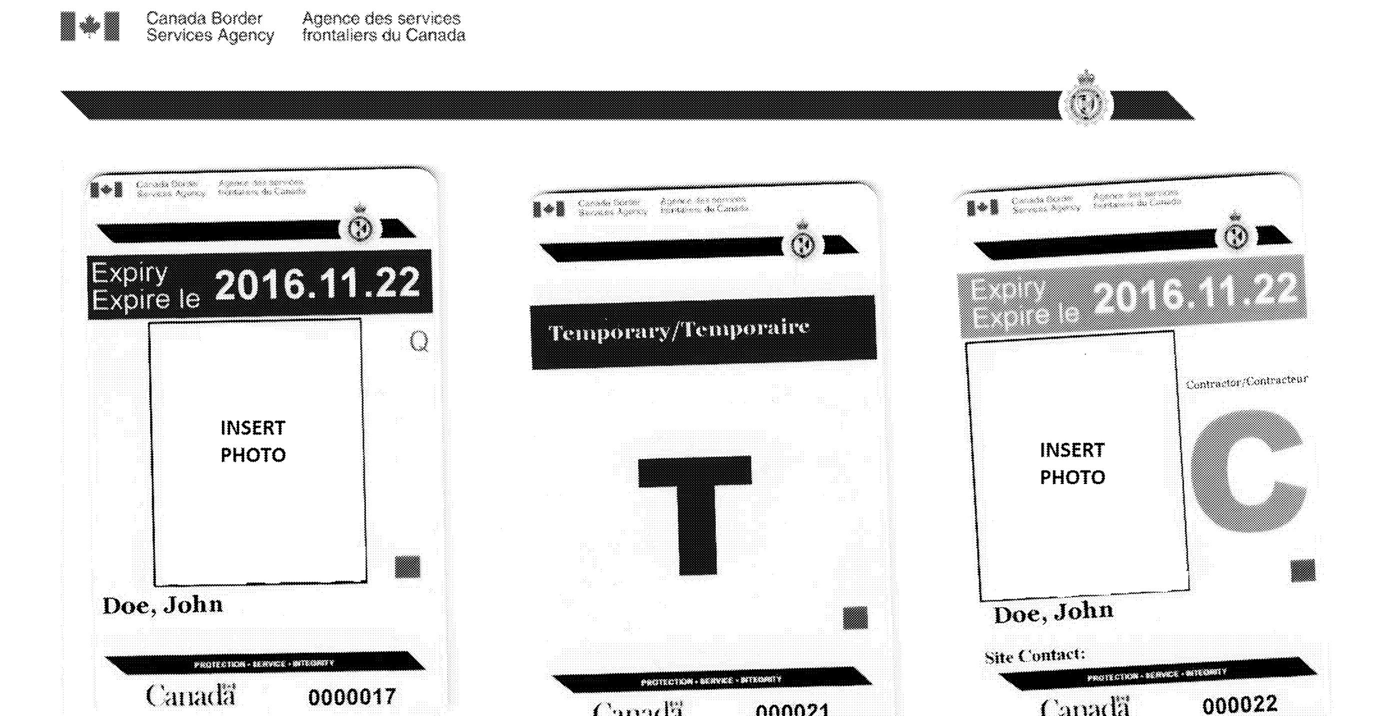
**New CBSA FIP Branded ID cards (reliability clearance)**

*(below are samples of photo ID cards issued by CBSA for employees who hold a valid RELIABILITY clearance)*




**New CBSA FIP Branded ID cards (secret clearance)**

*(below are samples of photo ID cards issued by CBSA for employees who hold a valid SECRET clearance)*



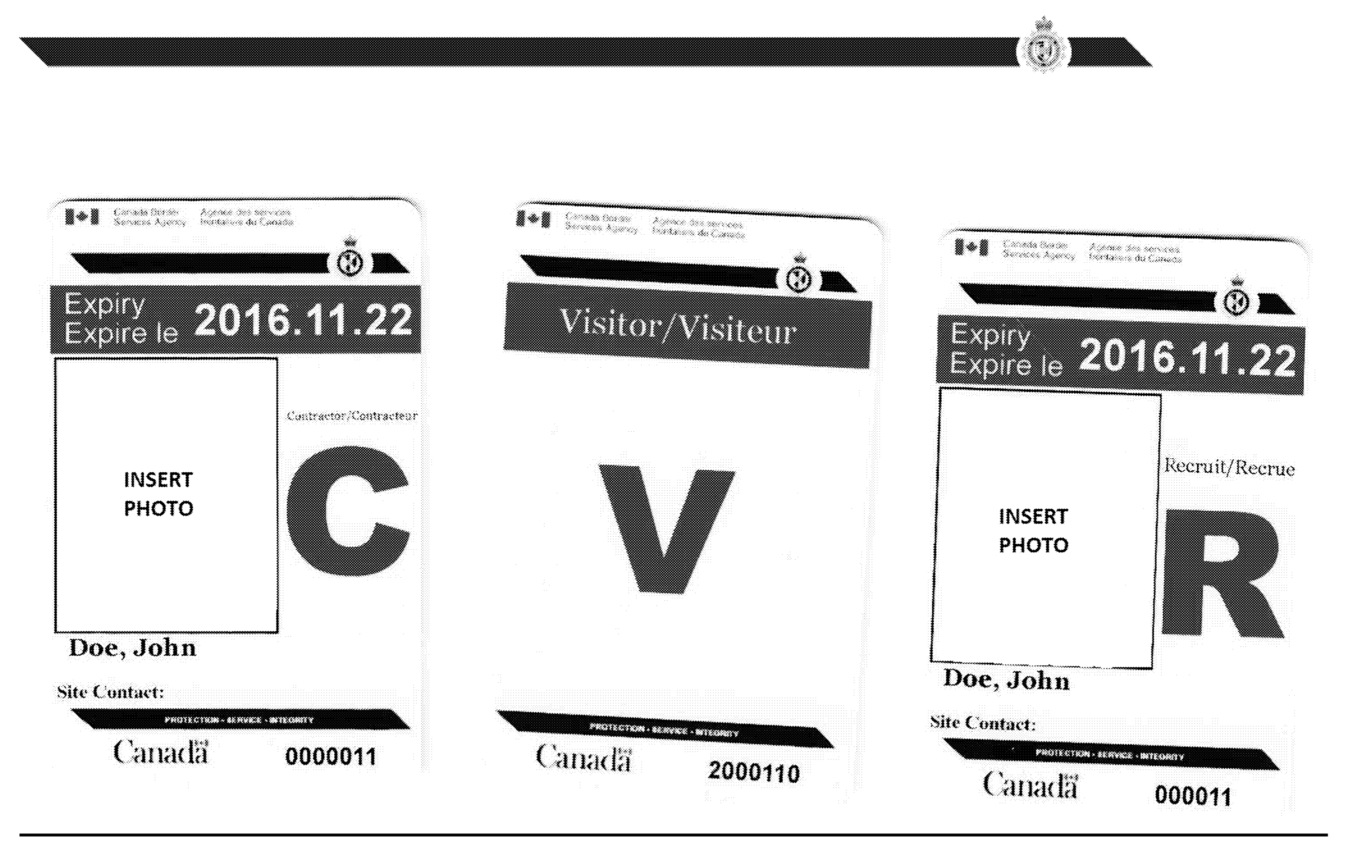

**New CBSA FIP Branded ID cards (Top secret clearance)**

*(below are samples of photo ID cards issued by CBSA for employees who hold a valid TOP SECRET clearance)*




**New CBSA FIP Branded ID cards (alternate Contractor, Visitor, Recruit)**

*(below are samples of photo ID cards issued by CBSA for employees who are Contractors, Visitors or Recruits)*




**New CBSA FIP Branded ID cards for temporary or part-time employees (who logically don't fit in any card categories above. "Q" is also for those who have access within the silent hours)**

*(below are samples of photo ID cards issued by CBSA for part-time or temporary employees)*

| Reliability | Secret | Top Secret |
| --- | --- | --- |
| Expiry / Expire le EPI_PERSON.State | Expiry / Expire le EPI_PERSON.State | Expiry / Expire le EPI_PERSON.State |
| Q | Q | Q |
| Photograph | Photograph | Photograph |
| [Last_Name]&', '&[First_Name] | [Last_Name]&', '&[First_Name] | [Last_Name]&', '&[First_Name] |
| Canada Card_Code | Canada Card_Code | Canada Card_Code |

Reliability Secret Top Secret

**New CBSA FIP Branded ID cards (Designation and Authority cards)**

*(below are samples of photo ID cards issued by CBSA for employees who are Designated and Authority)*



Agence des services frontaliers du Canada | Canada Border Services Agency



# Lignes directrices sur les cartes d'identité

PROTECTION • SERVICE • INTÉGRITÉ

Canada



# Table des matières



Ces lignes directrices entre en vigueur le 2 février 2015.

**Objet**

Le guide sur les biens contrôlés aux fins de la sécurité de l'Agence des services frontaliers du Canada (ASFC) décrit les cartes d'identité et les laissez-passer. Il a pour objet de réduire les risques d'accès non autorisé aux renseignements et aux biens de nature délicate.

**Champ d'application**

Le guide s'applique à tous les employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), aux contractuels et aux employés des agences privées ainsi qu'aux personnes en détachement ou affectées à l'ASFC (y compris les étudiants).

**Généralités**

Les cartes d'identité et les laissez-passer de l'ASFC doivent être portés en tout temps par les personnes qui se trouvent dans les locaux de l'ASFC et elles doivent être bien visibles. Échappent à cette règle les agents des services frontaliers en uniforme ou les personnes pour qui le port de la carte d'identité ou du laissez-passer représente un danger en matière de sécurité.

Le port de toute carte d'identité ou de tout laissez-passer particulier ne donne pas à son détenteur le droit de se soustraire aux mesures de sécurité matérielle ou aux contrôles d'accès de sécurité mis en place par le responsable des lieux. L'une des conditions de délivrance des cartes d'identité et des laissez-passer est que le détenteur respecte l'autorité légitime de la direction responsable des lieux auxquels il a accès et qu'il se prête aux contrôles de sécurité mis en œuvre.

Les cartes d'identité et les laissez-passer de l'ASFC sont la propriété de l'ASFC et ils ne doivent être utilisés qu'aux fins pour lesquelles ils ont été délivrés. Toute carte ou tout laissez-passer peut être révoqué, à la discrétion de la direction ou par le directeur de la Direction de l'infrastructure et de la sécurité de l'information (DISI).

À l'exception des laissez-passer de visiteur, aucune carte d'identité et aucun laissez-passer ne seront remis à quiconque ne dispose pas d'une autorisation de sécurité ou d'une cote de fiabilité valide.

Les demandes de carte d'identité ou de laissez-passer d'entrepreneurs doivent être accompagnées des documents appropriés comme le Formulaire des biens contrôlés (BSF208) dûment rempli et signé par le gestionnaire et l'employé.

La perte d'une carte d'identité ou d'un laissez-passer doit être signalée immédiatement à l'autorité de délivrance. Il est obligatoire de remplir le Formulaire de rapport d'incident relatif à la sécurité (BSF152). Une nouvelle carte est délivrée après le signalement de la perte de la carte d'identité à l'autorité de délivrance.







Les seuls modèles de carte d'identité et de laissez-passer autorisés sont ceux qui ont été envoyés par la Section de la sécurité matérielle, Direction de la sécurité et des normes professionnelles (DSNP), aux bureaux de la sécurité dans les régions et à l'Administration centrale et qui doivent être téléchargés dans tous les systèmes informatiques de cartes d'identité. Les modèles en question ne doivent pas être modifiés.

Les cartes d'identité, d'autorisation et de désignation sont produites au moyen des fichiers maîtres électroniques seulement. La surimpression des cartes, y compris l'application de la photographie de l'employé et des marques indiquant le niveau de sécurité, est également réalisée au moyen des fichiers maîtres électroniques que détiennent la Sécurité et les Normes professionnelles.

**Types de cartes d'identité et de laissez-passer**

Les cartes d'identité sont imprimées sur les cartes pré imprimées de l'ASFC fournies tandis que les laissez-passer (temporaire, de visiteur, de recrue et d'entrepreneur) sont imprimés sur les cartes blanches vierges. Des jetons d'accès supplémentaires permettant un accès aux locaux/aux immeubles conforme à la Norme opérationnelle pour le contrôle des accès seront requis.

**Carte d'identité à barre bleue :**

La carte d'identité à barre bleue se reconnaît à sa barre bleue qui renferme la date d'expiration de la carte et qui est placée au-dessus de la photo centrée. La carte d'identité à barre bleue est délivrée aux employés nommés pour une période indéterminée (permanents) de l'ASFC. Le détenteur de la carte a accès aux installations de l'ASFC partout au Canada, mais les procédures locales de contrôle d'accès doivent être respectées.

Les heures de fermeture doivent être inscrites sur la carte au moyen d'un « Q » rouge placé en haut à droite de la photo imprimée sur la carte. La cote de sécurité du détenteur de la carte est indiquée au moyen d'un carré de couleur en bas à droite de la photo (voir l'Annexe A – Légende des symboles).

**Laissez-passer temporaire :**

Le laissez-passer temporaire se reconnaît au « T » bleu qui figure au centre de la carte, elle-même traversée d'une barre bleue qui indique que l'employé est un employé nommé pour une période indéterminée. On trouve la cote de sécurité de l'employé au bas de la carte, à droite du « T ».

Le laissez-passer temporaire a été conçu principalement pour être remis aux employés de l'ASFC nommés pour une période indéterminée qui ont égaré ou oublié leur carte d'identité. Le laissez-passer ne doit pas quitter le site pour lequel il a été délivré et il doit être retourné au bureau qui l'a délivré à la fin de chaque visite. Il n'est pas nécessaire d'accompagner la personne munie d'un tel document.

**Laissez-passer de visiteur :**

Le laissez-passer de visiteur se reconnaît au « V » rouge et à la barre rouge qui renferme la date d'expiration de la carte. Le laissez-passer de visiteur est destiné aux personnes qui ne sont pas des employés de l'ASFC et qui



doivent accéder à un site ou à un bureau pendant une période d'au plus une journée. Quand elles entrent dans une zone d'accès restreint ou quand elles en sortent, ces personnes doivent toujours être accompagnées par un employé de l'ASFC qui dispose d'un accès autorisé. Le laissez-passer ne doit pas quitter le site pour lequel il a été délivré et il doit être retourné au bureau qui l'a délivré à la fin de chaque visite.

**Laissez-passer de recrue :**

Le laissez-passer de recrue se reconnaît au « R » rouge et à la barre rouge qui renferme la date d'expiration de la carte. Cette carte ne doit être utilisée que par le Collège de l'ASFC – campus principal (Rigaud, Québec) ou par les nouvelles recrues. Elle ne doit pas être utilisée dans une autre installation.

La cote de sécurité de la personne est indiquée au moyen d'un carré de couleur en bas à droite de la photo (voir l'Annexe A – Légende des symboles).

**Laissez-passer d'entrepreneur :**

Deux cartes d'entrepreneur seront utilisées.

1. La carte d'entrepreneur pour les ressources contractuelles et les consultants

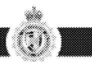
La carte d'entrepreneur sur laquelle on trouve un « C » vert et une barre verte renfermant la date d'expiration de la carte sert à identifier les ressources contractuelles/consultants. Le prêt de la carte d'entrepreneur est inscrit au registre, mais celle-ci n'est rendue qu'au moment de l'échéance du marché. La personne-ressource sur le site de l'ASFC (gestionnaire/superviseur/agent de sécurité) doit être clairement indiquée sur le laissez-passer. La carte d'entrepreneur des ressources contractuelles/consultants peut demeurer en la possession du consultant jusqu'à la fin de son contrat. Il n'est pas nécessaire d'accompagner les entrepreneurs suivant leur cote de sécurité et la zone d'entrée.

Les cartes d'entrepreneur sont délivrées à chaque entrepreneur, et des photographies doivent figurer sur chaque carte afin d'identifier les personnes. La cote de sécurité de l'entrepreneur est aussi indiquée en bas à droite du « C » vert.

2. Gens de métier

La carte d'entrepreneur pour ce type de personnel se reconnaît au « C » rouge et à la barre rouge qui renferme la date d'expiration de la carte. Quand il entre dans une zone d'accès restreint ou quand il en sort, l'entrepreneur doit toujours être accompagné par un employé de l'ASFC qui dispose d'un accès autorisé. La carte d'entrepreneur des gens de métier contractuels doit chaque jour être inscrite au registre pendant toute la durée du marché. La personne-ressource sur le site de l'ASFC doit être clairement identifiée sur le laissez-passer. Le laissez-passer ne doit pas quitter le site pour lequel il a été délivré et il doit être retourné au bureau qui l'a délivré à la fin de chaque visite.

**Carte d'identité à barre verte pour employés temporaires ou temps-partiel**:



La carte d'identité à barre verte se reconnaît à sa barre verte qui renferme la date d'expiration de la carte et qui est placée au-dessus de la photo centrée, **sans le « C »**. La carte d'identité à barre verte est délivrée aux employés nommés **temporaires ou temps-partiel** incluant par exemple : nommés pour une période déterminée, occasionnels et à temps partiel ou il y a une relation employé/employeur mais pas sur une base à temps plein. Ceci inclus aussi les étudiants, étudiants coop cependant cela **n'inclue pas** les recrues tel que définis ci-dessus. Le détenteur de la carte a accès aux installations de l'ASFC partout au Canada, mais les procédures locales de contrôle d'accès doivent être respectées.

Les heures de fermeture doivent être inscrites sur la carte au moyen d'un « Q » rouge placé en haut à droite de la photo imprimée sur la carte. La cote de sécurité du détenteur de la carte est indiquée au moyen d'un carré de couleur en bas à droite de la photo (voir l'Annexe A – Légende des symboles).

## Cartes de désignation et d'autorisation

Pour obtenir de plus amples renseignements sur les cartes de désignation et d'autorisation, consultez le Manuel de l'exécution de l'ASFC, partie 8, Formulaires servant à l'exécution de la loi.

### 1 Responsabilités

L'autorité déléguée de délivrance de l'ASFC est responsable de la délivrance, du contrôle et de la récupération des cartes d'identité et des laissez-passer. La Sécurité régionale ou, à l'Administration centrale, la Section de la sécurité à l'Administration centrale, est l'autorité de délivrance. Toutes deux peuvent approuver la délégation à des personnes qui doivent délivrer les cartes et les laissez-passer (p. ex. les commissionnaires).

### 2 Sensibilisation des employés

Les employés doivent informer leur superviseur lorsqu'ils s'aperçoivent que des personnes sans carte d'identité ou sans laissez-passer, non accompagnées par un membre du personnel de l'ASFC, ou munies d'une carte expirée se trouvent dans une zone opérationnelle de l'ASFC. Le superviseur en informera ensuite la Sécurité régionale ou la Sécurité de l'Administration centrale.

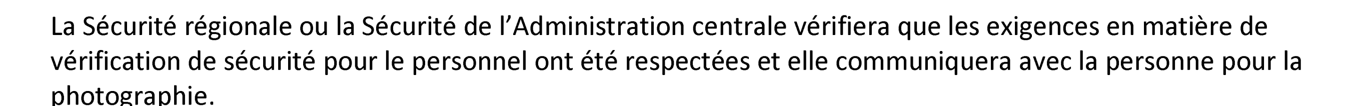
## 3 Procédures

## 3.1 Délivrance

Les cartes d'identité ne doivent être délivrées qu'aux personnes qui ont satisfait aux exigences de l'ASFC en matière de vérification de sécurité pour le personnel. Cette procédure doit être suivie avant que les personnes n'entrent en fonctions.

Le gestionnaire ou son remplaçant remplira le Formulaire de biens contrôlés (BSF208) et le transmettra à la Sécurité régionale ou à la Sécurité de l'Administration centrale à des fins de traitement.



La Sécurité régionale ou la Sécurité de l'Administration centrale vérifiera que les exigences en matière de vérification de sécurité pour le personnel ont été respectées et elle communiquera avec la personne pour la photographie.

Une fois la photo prise et la carte prête, l'employé et l'autorité de délivrance de l'ASFC signeront le Formulaire de biens contrôlés (BSF208). Le formulaire BSF208 dûment rempli sera conservé au bureau de la Sécurité régionale ou de la Sécurité de l'Administration centrale. (Cela peut être coordonné dans les régions).

Les cartes d'identité doivent être remises avec un étui en plastique et un cordon. Les cartes d'identité doivent être fabriquées à l'aide des cartes pré imprimées ou des modèles fournis par la Section de la sécurité matérielle (SSM). Les laissez-passer doivent être fabriqués à l'aide de la carte vierge et du modèle fournis par la SSM.

Le laissez-passer de visiteur/temporaire ne doit pas quitter le site pour lequel il a été délivré et il doit être retourné au bureau qui l'a délivré à la fin de chaque visite. Avant de délivrer un laissez-passer, l'autorité de délivrance devra vérifier l'identité de la personne en examinant sa pièce d'identité avec photo délivrée par le gouvernement fédéral ou provincial. Tous les entrepreneurs qui se présentent dans les bureaux de l'ASFC et qui n'ont pas de carte officielle d'entrepreneur de l'ASFC doivent obtenir une carte de visiteur et être accompagnés en tout temps. Un registre de contrôle doit être utilisé pour inscrire les renseignements suivants :

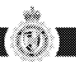
- L'adresse de l'installation;
- Le nom de la personne;
- Le numéro d'identification du laissez-passer;
- Le numéro d'identification personnel de la personne (tiré d'une pièce d'identité avec photographie)
- La date/l'heure de délivrance;
- Le nom de la personne qui l'a délivré;
- La date/l'heure où a été récupérée la carte;
- Le nom de la personne qui a récupéré la carte;
- La personne-ressource sur le site de l'ASFC responsable du visiteur.

Les registres doivent être entreposés dans une armoire approuvée, ainsi que les laissez-passer de visiteur/temporaires lorsqu'ils ne sont pas utilisés. Les registres doivent être conservés à des fins de vérification.

Un laissez-passer d'entrepreneur ne peut être délivré que lorsqu'il a été démontré que l'entrepreneur satisfait aux exigences de sécurité définies dans le marché. La Liste de vérification des exigences relatives à la sécurité (LVERS) fournit la méthode qui fait autorité pour déterminer le niveau de vérification de sécurité à utiliser.

Le gestionnaire ou le chargé de projet remplira le Formulaire de biens contrôlés (BSF208) et le transmettra à la Sécurité régionale ou à la Sécurité de l'Administration centrale à des fins de traitement. Le formulaire BSF208 devra être conservé par la Sécurité régionale ou la Sécurité de l'Administration centrale.

La Sécurité régionale ou la Sécurité de l'Administration centrale vérifiera que les exigences en matière de vérification de sécurité ont été respectées et elle communiquera avec l'entrepreneur ou le chargé de projet pour prendre des dispositions pour la photographie.



La Sécurité régionale ou la Sécurité de l'Administration centrale remettra les laissez-passer d'entrepreneur au chargé de projet ou au gestionnaire; le chargé de projet, le gestionnaire ou son délégué, délivrera un laissez-passer après avoir vérifié l'identité de la personne en examinant sa pièce d'identité avec photo délivrée par le gouvernement fédéral ou provincial. Un registre de contrôle doit être utilisé pour inscrire les renseignements suivants :

- L'adresse de l'installation;
- Le nom de l'entrepreneur;
- Le nom de l'entreprise pour laquelle il travaille;
- La date/l'heure de la délivrance;
- Le nom de la personne qui l'a délivré;
- La date/l'heure où a été récupérée la carte;
- Le nom de la personne qui a récupéré la carte;
- La personne-ressource sur le site de l'ASFC qui est responsable du visiteur.

Le laissez-passer d'entrepreneur (laissez-passer rouge marqué d'un « C » conformément à l'annexe B) ne doit pas quitter le site pour lequel il a été délivré et il doit être retourné au bureau qui l'a délivré à la fin de chaque visite. On peut délivrer une carte d'entrepreneur (laissez-passer vert marqué d'un « C » conformément à l'annexe B) aux employés qui ne travaillent pas pour l'ASFC et qui exécutent, dans le cadre d'un marché, des travaux pour l'Agence ou pour le compte de l'Agence et leur accorder le privilège de ne pas devoir signer à l'entrée et à la sortie le registre de contrôle, à la discrétion du gestionnaire régional de la sécurité ou du gestionnaire de la sécurité à l'Administration centrale. Le chargé de projet ou le gestionnaire retournera tous les laissez-passer d'entrepreneur (laissez-passer vert marqué d'un « C ») à la Sécurité régionale ou à la Sécurité de l'Administration centrale à l'achèvement des travaux prévus par le marché ou en cas d'expiration du laissez-passer.

## 3.2 Photographies

Les photographies des cartes d'identité et des laissez-passer doivent respecter les normes suivantes :

- La photo doit être claire, bien définie et bien centrée;
- L'arrière-plan doit être bleu clair et sans ombrage;
- La photo doit montrer le visage complet de face et les épaules, qui doivent être centrés sur la photo et bien en face de la caméra;
- Les yeux doivent être ouverts et clairement visibles et ils ne doivent pas être rouges;
- Les lunettes, y compris les lunettes de vue teintées, peuvent être portées dans la mesure où les yeux sont clairement visibles; les lunettes de soleil ne sont pas acceptées;
- L'expression faciale doit être neutre (pas de froncement de sourcils ni de sourire) et la bouche doit être fermée;
- Les chapeaux et les couvre-chefs ne sont pas permis, à moins d'être portés pour des raisons religieuses ou médicales et seulement s'ils laissent voir entièrement les traits du visage;
- Les photos doivent être sauvegardées dans le format jpeg, en utilisant le nom de famille, le prénom et l'année de la photo, p. ex. Doe, Jane, 2011;



- Les photos doivent être prises à nouveau tous les cinq (5) ans ou lorsque des traits d'identification importants ont changé.

### 3.3 Retour de la carte d'identité

Les cartes d'identité doivent être retournées au bureau de la Sécurité régionale ou de la Sécurité de l'Administration centrale au moyen du Formulaire de biens contrôlés (BSF208) et du Formulaire de départ d'un employé (BSF270).

Les retours sont nécessaires dans les cas suivants :

- L'employé cesse d'être un employé de l'Agence;
- La carte a expiré;
- La personne cesse d'être employée à l'endroit pour lequel la carte d'identité a été délivrée;
- Dans des cas extrêmes, lorsqu'il existe une menace immédiate (c.-à-d. violence en milieu de travail) et sur demande de la direction responsable des lieux auxquels la personne a accès ou sur demande d'un membre de l'organisation de la Sécurité matérielle lorsqu'il agit sous l'autorité de l'agent de sécurité du ministère;
- L'employé va s'absenter temporairement pendant une période de plus de quatre mois de son poste lui donnant droit à la carte d'identité.

## 4 Perte ou vol

Il est indispensable de signaler immédiatement la perte ou le vol de cartes d'identité afin d'éviter toute compromission ou de diminuer le risque de compromission. Le détenteur de la carte d'identité doit remplir le Formulaire de rapport d'incident relatif à la sécurité (BSF152) et remplir le Formulaire de biens contrôlés (BSF208) afin de signaler la perte ou le vol de sa carte d'identité. Le formulaire BSF152 doit être signé par le directeur de l'employé et envoyé à la Sécurité régionale ou à la Sécurité de l'Administration centrale. Le Formulaire de biens contrôlés (BSF208) dûment rempli doit être joint au formulaire BSF152 pour la délivrance d'une carte d'identité de remplacement.

## 5 Destruction

Les cartes d'identité et les laissez-passer seront détruits par la Sécurité régionale ou la Sécurité de l'Administration centrale seulement. Le renvoi des cartes d'identité et des laissez-passer aux fins de destruction est essentiel dans le processus de contrôle.

## 6 Processus de responsabilisation

L'application des lignes directrices sera contrôlée au moyen d'inspections de sécurité qui seront effectuées par la Direction de la sécurité et des normes professionnelles, la Sécurité régionale ou la Sécurité de l'Administration centrale, et au moyen de ratissages de sécurité effectués par des agents de sécurité régionaux et par des agents de sécurité de l'Administration centrale.



La Direction de la vérification interne et de l'évaluation des programmes de la Direction générale des services intégrés (DGSI) offrira un niveau d'assurance indépendant en effectuant des vérifications internes.

## 7 Personne-ressource pour les mises à jour

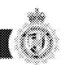
Quiconque souhaite obtenir des éclaircissements sur ce document ou une version mise à jour doit communiquer avec le bureau de la Sécurité régionale ou de la Sécurité à l'Administration centrale ou avec le gestionnaire, Section de la sécurité matérielle, Direction de la sécurité et des normes professionnelles (DSNP)

## 8 Écart par rapport à la norme

Tout écart par rapport à la norme doit être approuvé par la Section de la sécurité matérielle de l'AC.

Pour tout éclaircissement supplémentaire, veuillez communiquer avec le gestionnaire de la DSNP, Sécurité matérielle (Administration centrale-Ottawa), à l'adresse suivante : CBSADSOSecurity@cbsa-asfc.gc.ca

Gestionnaire, Sécurité matérielle, AC



# Annexe A

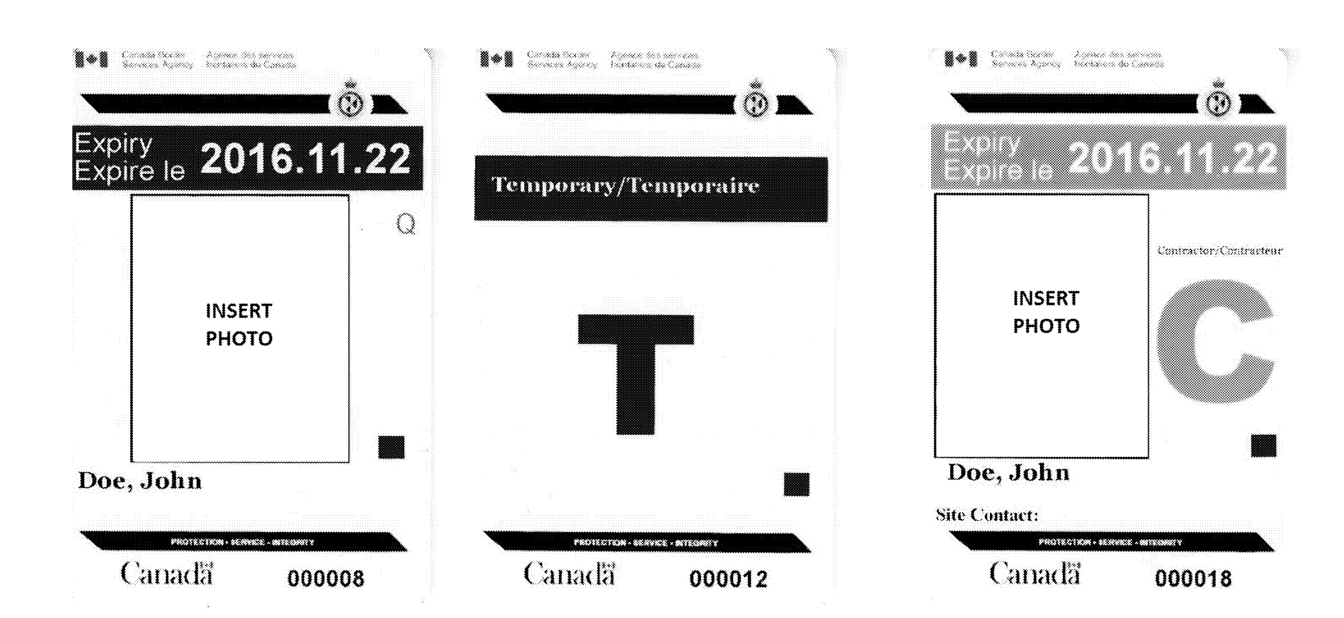
## Légende des symboles

Fiabilité
Secret
Très secret
Heures de fermeture Q

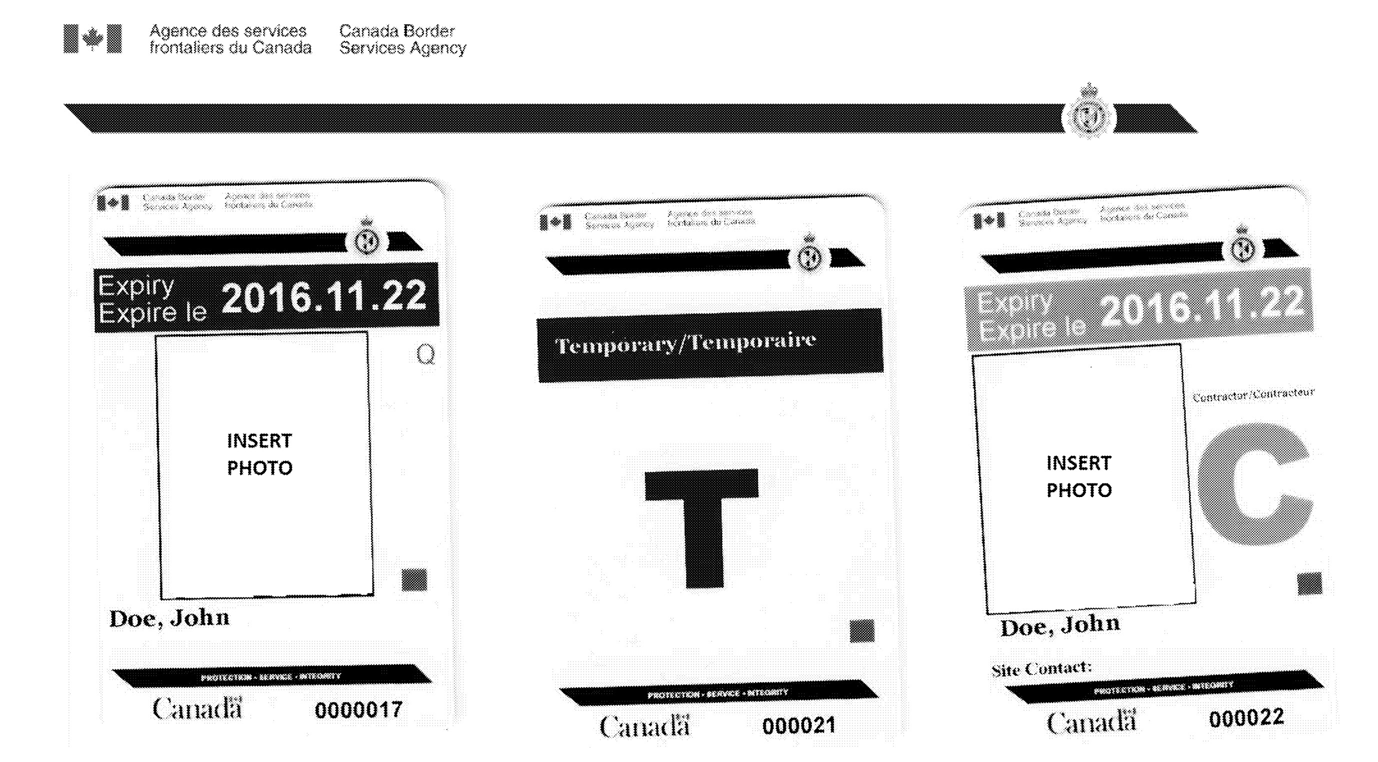


# Annexe B

**Nouvelles cartes d'identité de l'ASFC dans le cadre du PCIM (cote de fiabilité)**
*(le modèle ci-dessous est une carte d'identité produit par l'ASFC pour les employés qui tiennent une côte de fiabilité valide)*

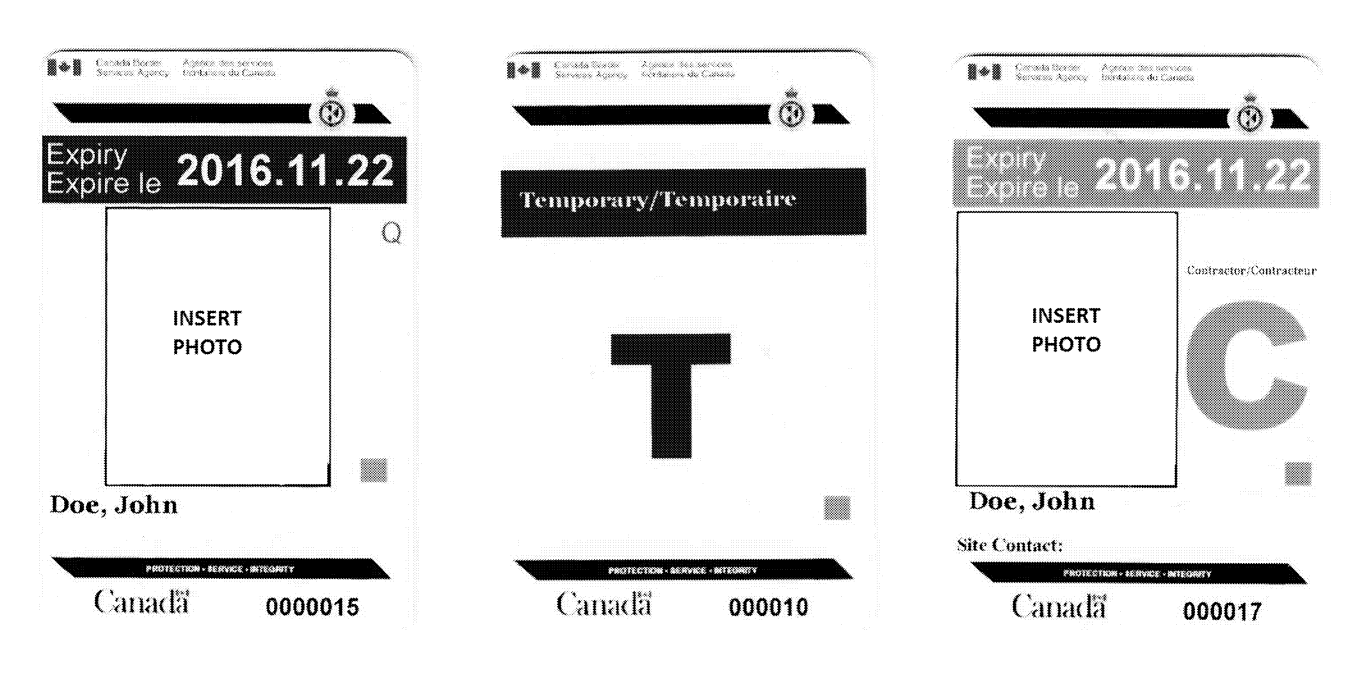



**Nouvelles cartes d'identité de l'ASFC dans le cadre du PCIM (cote de niveau Secret)**
*(le modèle ci-dessous est une carte d'identité produit par l'ASFC pour les employés qui tiennent une côte de niveau Secret valide)*




**Nouvelles cartes d'identité de l'ASFC dans le cadre du PCIM (cote de niveau Très secret)**

*(le modèle ci-dessous est une carte d'identité produit par l'ASFC pour les employés qui tiennent une côte de niveau Très secret valide)*



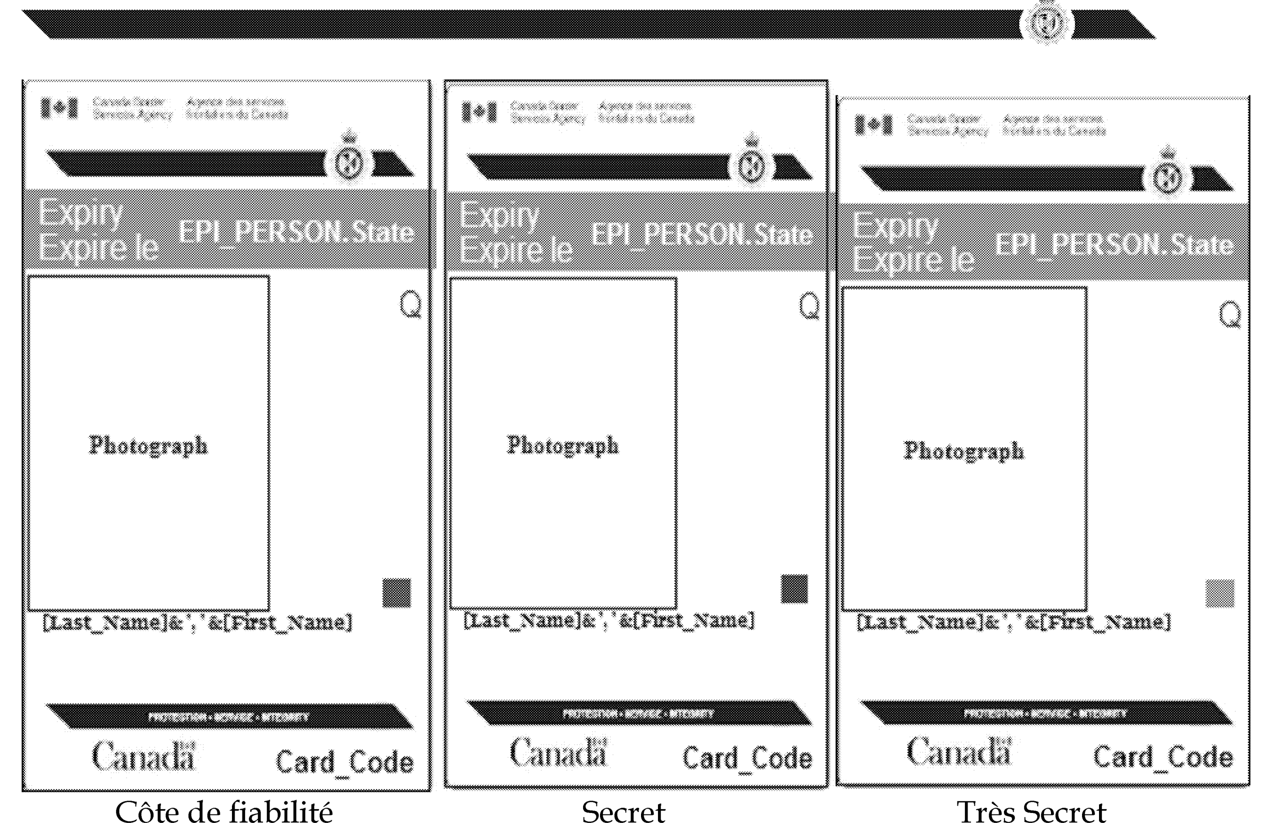




**Nouvelles cartes d'identité de l'ASFC dans le cadre du PCIM (autre entrepreneur, visiteur, recrue)**
*(le modèle ci-dessous est une carte d'identité produit par l'ASFC pour les employés qui sont Entrepreneur, visiteur, recrue, etc.)*




**Nouvelles cartes d'identités de l'ASFC dans le cadre du PCIM pour les employés temporaires ou temps-partiel (qui, logiquement, ne font pas partie des autres catégories de cartes ci-dessus. "Q" est aussi pour ceux qui ont accès durant les heures de fermeture)**
*(le modèle ci-dessous est une carte d'identité produit par l'ASFC pour les employés temporaires ou temps-partiel)*




Côte de fiabilité    Secret    Très Secret

**Nouvelles cartes d'identité de l'ASFC dans le cadre du PCIM (cartes de désignation et d'autorisation)**

*(le modèle ci-dessous est une carte d'identité produit par l'ASFC pour les employés de désignation et d'autorisation)*



Canada Border Services Agency    Agence des services frontaliers du Canada



# Standard for Physical Security in Remote or Isolated Areas

PROTECTION • SERVICE • INTEGRITY





This Standard takes effect on February 2, 2015.

**Purpose**

1. This standard provides guidance with respect to activities associated with the conceptualization, design and implementation of physical security controls taking into account higher risk areas, areas of isolation or where an effective response may not be possible. This standard includes requirements (indicated by *must, shall, or will*) and recommendations (indicated by *should, might, or may*).

**Intent**

2. The intent of this document will provide clear, concise guidance with respect to the various requirements of the Physical Security to those involved in the following:
    a. Travel to areas which do not have the infrastructure or services necessary to respond quickly (under 24 hrs) to security-related events or issues of personal security,
    b. Travel to locations that are at a moderate to high probability of major events that may cause the destruction or disruption of services or infrastructure making a response more difficult,
    c. Travel to locations where the level of trust in first responders may be called into question, leaving an individual at higher risk.
    d. These environments may reside within Canada (isolated posts or environs) or abroad (countries in which Canada's national presence is limited). They may also emerge as the result of natural disasters (at home or abroad) which destroys or disrupts the infrastructure needed to mount an effective response. The guidance provided here should be taken in light of the particular circumstances in which personnel find themselves or in which personnel may find themselves.
3. This standard is meant to be read in conjunction with the other Physical Security standards but is intended to provide guidance unique in that those standards assume that the services and infrastructure necessary to respond are within the area and can be trusted to respond. When reading the other standards, the intent of those standards should be taken describing the security goal to be achieved.

**Scope**

4. This standard pertains to all Agency-related activities where there is a need to take reasonable steps to protect personnel, sensitive assets (including information) or operations.

**Requirements**







*General*

5. Those planning operations or activities must take into account the ability to respond to a range of physical security threats. Before any such travel is undertaken, the management responsible must have conducted an assessment to determine not only the physical security risks to assets and information, but also in terms of the personal safety and security.
6. In conducting those assessments, the travel is to take into account the threat environment present and likely to emerge in the operating environment:
    a. any operations that take place in locales under travel advisories (official advisories such as those put out by the Department of Foreign Affairs and Trade Development, the USA Bureau of Consular Affairs, or similar official source) or considered to be a HIGH threat environment must ensure that any plans associated with the evacuation or repatriation of the individual and sensitive assets includes consideration if infrastructure or services from outside the Agency can no longer be counted upon; or
    b. any operations that take place in locales that are known or reasonably suspected to be difficult in terms of communications or access (including rescue) should ensure that they have taken into account the ability to assure communications from the individual and have in place plans that would allow for the retrieval of personnel and sensitive assets.

7. In the context of these kinds of operations, the focus must emphasize preparation, prevention, containment and response. These are to be taken as meaning the following:
    a. **Preparation** – in terms of personal preparation, ranging from the duty to inform the individual of risks that they may face and training that is suitable to mitigating aspects of those risks (such as hostile environment training, survival training, close protection techniques, etc.);
    b. **Prevention** – in terms of physical, procedural, technical or administrative controls that are intended to ensure that the person, asset, or operation is protected from harm to the extent;
    c. **Containment** – in terms of those immediate steps that are taken upon discovery that an individual or sensitive asset is at an unacceptable level of risk;
    d. **Response** – in terms of those coordinated and managed steps that are taken in order to move past containment and into a state in which operations can resume; and
    e. *The core difference between containment and response is that containment is described in terms of goals to be achieved and under the immediate control of the Officer involved while the response is a managed activity that takes certain pre-determined steps to complete tasks or achieve those goals. For example, upon discovering a bomb near the car, the Officer's containment may be to move out of the area quickly (containing the risk for personal injury) and communicating with the appropriate point of contact so that management is informed of the issue. The response may be management shifting the operations to a backup location or to put a hold on the operations, depending on the situation.*







8. Where individuals are being considered for operations in these circumstances (in Remote and Isolated Areas), they are to be assessed in terms of the following. Note that this assessment method is not used to evaluate the performance or work capacity of the individual but is intended only to assist in the physical security risk assessment process:
    a. **Hard targets** – those who are aware of the risks, have been trained to deal with the most probable security threats in the area (such as a natural disaster), have taken steps to mitigate those risks (such as vaccinations), and that are capable of sustaining their own activities for not more than 96 hours. Those designated as hard targets likely have previous training or experience operating in difficult or complex environments.
    b. **Moderate Targets** – those that are aware of the risks, are made familiar with common techniques on addressing those risks and have a capability of maintaining their own operations for up to 48 hours. Those designated as being moderate targets may have had limited training or past experience operating in foreign, but not difficult or complex, environments, and
    c. **Soft Targets** – those that are aware of the risks, are familiar but not fully trained in dealing with the most probable threats in the area and that would require support to maintain themselves for up to 48 hours. Those designated as being soft targets are not likely to have had previous training or experience operating outside of Canada or friendly nations.

**Methodologies and Specific Guidance**

*Preparation*

*Assessment of Risk*

9. The preparation for these kinds of operations must take into account reasonably foreseeable risks and should make reasonable attempts to determine the following:
    a. **Deliberate threats** – as provided by CSIS briefings, law enforcement briefings, and other intelligence regarding threats associated with terrorism, organized crime, local crime, and corruption,
    b. **Accidental threats** – as provided by open source research (contact the Physical Security section) and including warnings associated with traffic accidents, construction standards (or lack thereof), and local customs that may become a source of conflict, and
    c. **Natural** – as provided by various Emergency management databases, weather services, the World Health Organization and travel organizations (specifically flora and fauna).
10. Even if an assessment of risk is conducted, the individual should be advised to maintain a level of awareness through travel advisories and other sources of official information up to and including the point of departure.
11. For all environments, it is recommended that an itinerary is prepared with call-in points (such as points for departure, arrival at city, cleared customs, depart for local site, at local site, etc.) and with a plan that details the likely arrival times at each point. For higher risk areas, this plan should also include a plan that identifies conditions where the individual misses a pre-arranged check in. In







higher threat environments, such itineraries should also include a *duress word* that can be used to covertly advise an individual that the Officer is in need of assistance but unable to ask for such assistance overtly. Instructions for times where communications are not available should be predetermined.

*Recommendation for Specialized Training*

12. Where it is determined that an individual may be at risk in terms of personal safety, consideration should be given to ensuring that the individual attends the appropriate hostile training courses.
    a. In cases of **conflict**, consideration should be given to the *hostile environment training* or similar personal protection / safety provided government institutions as appropriate (DND for conflict, CSIS for personal safety, etc.);
    b. In cases of **natural disaster or harsh environments**, consideration should be given to basic survival training and advanced first aid training;
    c. In cases where there is a risk of disease or contagion, consideration should be given to a briefing through the World Health Organization's representative with respect to steps that should be taken to reduce any such risks; and
    d. It should be noted that discussions are commencing with respect to the above to attempt to ensure a level of availability.

*Limiting Exposure of Sensitive Assets*

13. When considering this kind of travel, consideration should be given to limiting the exposure of sensitive assets. This should balance the need for the assets for operational purposes, the sustainability of the individual in the field and the potential for exposure of the assets.
    a. For **telecommunication devices**, individuals must take into account the guidance provided by the Communications Security Establishment of Canada (CSEC) with respect to the protection of mobile communications devices and computers (laptops),
    b. Where **controlled assets** are involved, the serial number of the asset must be recorded with the manager responsible for the program with a copy to the National Coordinator Security Controlled Assets (if a security controlled asset). Regional security should also be informed.
        i. *Outside of Canada* - Unless the Agency has directly and specifically authorized the use of the controlled asset, it must remain secured in Canada. Security controlled assets should, wherever possible, be moved only through diplomatic pouches,
        ii. *Inside of Canada* – Controlled assets, except identification cards or badges, should remain with the assigned Port of Entry (as for example Port Stamps, Arming).
    c. Where **facilities** are proposed, these should be arranged through organizations with an understanding of the environment:
        i. *For international travel*, the nearest Canadian mission with a clear description of any potential work that may be done,







ii. *For domestic travel*, trusted entities or travel coordinators with a direct knowledge of the location and its environment. Ideally, contact should be established with local personnel (or at least those with experience in the local environment) to determine these kinds of considerations, and

d. Where **long term arrangements** are being proposed, the identification of trustworthy food and water sources should be sought from the local mission.

*e. It is strongly recommended that, before setting out, management conduct an evaluation of all Agency assets that are being proposed for movement to the foreign environment in order to determine (1) the need for the asset to be taken and (2) the potential for compromise (through practices such as reverse engineering) of Agency related processes or methods should the tools fall outside of Agency control.*

*f. It is strongly recommended that management also confirm any arrangements with allied nations that may be used in cases where the Officer needs to be removed from areas posing immediate and grave risk. It should be noted that care must be used with respect to discussions should those nations be involved in competitive positions.*

*Limitation of Personal Information and Backup of Personal Information*

14. It is strongly recommended that individuals take steps to protect and limit the exposure of personal information when abroad. This may be combined with a contingency plan to include a scanned page of a passport, visa, and vaccination book that is uploaded to a secured cloud (double password protect). While this step may appear counter-intuitive, the intent of this step is to reduce the risks associated with being able to establish identification should those documents be lost.

15. It is strongly recommended that individuals have signed for and received any medic alert tags or similar items that can identify allergies and other conditions as medical records may or may not be available. This information should also be provided to management (for domestic and international travel) and the nearest Canadian mission (where the activity is being registered abroad),

16. It is strongly recommended that personnel ensure that all contact information (work, emergency contacts at work, and family emergency contact information) is up-to-date and that all legal documents (insurance, etc.) are located before setting out.
    a. One of the major sources of stress or distraction while away on these kinds of assignments is the family-related issues that may persist into the trip. As these distractions may result in a loss of attention to detail that leaves the individual vulnerable in unfamiliar surroundings, it is strongly recommended that part of the preparatory routines include ensuring that banking, payments, school-related issues, and other similar family obligations are addressed to the extent possible; and
    b. Ensure that the family is briefed with respect to the means of communication and the services available through the Canadian mission.

*Travel Kit*







17. It is recommended that each individual be advised to have a travel kit that can be carried on the person at all times. It is proposed that this kit include the following for missions abroad:
    a. Copies of all core documentation (passport, visa, vaccination, travel authorization document) in a watertight pouch;
    b. Copies of any prescriptions (ensuring that they are clearly legible) with at least 72 hours of such medication;
    c. Emergency contact information, taking into account that such contact information should be to the nearest Canadian Mission or the DFATD traveller hotline. Information for this can be found through the DFATD website at http://travel.gc.ca/assistance/emergency-assistance
    d. Water purification tablets;
    e. 48 hours of high-energy food bars if food can be transported legitimately (if not, purchase sealed items once clear of customs);
    f. Marker with waterproof paper; and
    g. Appropriate clothing for the climate.

18. It is recommended that those proceeding on assignments into remote areas ensure that they maintain 72 to 96 hours of ability to maintain heat, water, food, and shelter. Additional resources to maintain communications which do not rely on land-based infrastructure should also be given consideration, particularly in areas with limited or no cellular or similar communication.

19. It is further recommended that individuals maintain a small amount of currency secured in two locations on the body so as to have a cash reserve. It should be clear to persons that the electronic financial transaction systems in many countries are not to the same standard as those in North America.
    a. In certain countries, it may be warranted to have a pre-paid debit card (not tied to any bank accounts) holding an appropriate amount that can be used for transactions in order to limit the exposure of personal bank accounts to various forms of electronic compromise.

*Route Planning*

20. Personnel in transit are often subject to a range of threats that may include deliberate hostile threats to natural events. For this reason, those operating in remote or isolated areas should incorporate the following into their route planning:
    a. Always have an itinerary and communicate it to the point of contact at the destination and copy (if possible) management. There should always be two trusted parties aware of your location and activities at all times,
    b. In higher threat areas, remain aware of areas that have higher crime rates, are subject to disruption due to protests, prone to natural disasters or events, etc.,
    c. In higher threat areas, vary the routes, times of departure and, if possible, the vehicle used in order to throw off persons that may be seeking to establish your patterns of behaviour for planning purposes,







d. Along the route, have break-off points that you can use to quickly bypass obstacles or disruptions. If travelling down isolated routes, be aware of turnoff areas, runaway lanes and similar kinds of routes,
e. Avoid bottlenecks or areas of high-traffic congestion as these may offer opportunities for criminal activity (ranging from carjacking to smash-and-grabs). This also includes having an awareness of areas which are subject to restrictions due to climatic conditions,
f. Always leave your vehicle in a secure location or under the observation of a trustworthy (coordinated or approved by the mission in the area) entity. Before setting out, do a quick circle check for the condition of tires, wheel-wells or signs of leakage under the vehicle,
g. At the end of each transit, check fuel and fluids to ensure that the vehicle is ready for the next movement,
h. If renting a vehicle, do not book in advance and switch vehicles periodically; and
i. Never leave registration or sensitive material (assets, information) in the vehicle unless in a locked box secured in the trunk if necessary to leave items in the vehicle. Agency assets are not to be left unattended exposed on seats, between seats, or in locations that are in plain view.

*Prevention*

21. The key to prevention is to ensure that employees are both aware and vigilant on one hand and, on the other hand, all arrangements are to be made through trusted (mission) parties.

22. When considering preventive measures, the following should be considered:
    a. Having the individuals met at Customs by an individual identified from the opposite party and coordinated through mutually trusted channels,
    b. Only using vehicles that are arranged through the mission,
    c. Only using communication devices provided by the Agency for official communications and in accordance with the direction provided through the Information Security and IT Security organizations,
    d. Ensuring that any personal valuables are secured at home or at the mission, not on the person,
    e. Only using portable media storage devices that use Agency approved encryption and in accordance with the guidance provided by the Information Security and IT Security organizations.
        i. In higher threat areas where such devices are absolutely necessary, it is strongly recommended that the device also have the capability to be wiped remotely should it be lost or fall outside of control.
    f. Ensuring that clothing and similar materials are suitable to the environment but also to the prevention of exposure to various forms of disease or contamination. Take into account the possibility and probability of changes in weather up to and including extreme inclement weather as appropriate to the region,







g. Ensuring adequate time for vaccinations or similar medical controls to take effect,
h. *It should be noted that in environments where there is a significant competitive aspect to the operations (such as for trade purposes, etc.), it is possible that hotel rooms or similar accommodations will be entered by those seeking to gain advantage. In these cases, personnel should not consider locked luggage to be secure or a do not disturb sign to be adequate deterrence.*

*Containment*

23. Containment refers, as indicated above, to the steps that are taken as an immediate and near-instinctive reaction to the discovery of an event. They are not considered part of the response but are intended to ensure that the individual is able to re-establish having the initiative in the situation and has the opportunity to assess the situation and trigger an appropriate response.
    a. For personnel, the goal is to be able to detect suspicious or potentially hostile events. In this case, the priority is to remove one's self to a safe location. Safe locations should be identified along common routes or near work areas that can be moved to quickly and without major coordination.
    b. For personnel, it is important to understand that employees or representatives of the Agency are watched and observed by a range of entities. It is therefore recommended that, while it is certainly possible to experience the local culture and take away other benefits from these kinds of assignments, that such activities should be tempered with moderation and planned in such a way as not to leave the individual vulnerable to various forms of compromise (ranging from kidnapping, criminal activity, sexual assault, or various forms of extortion / coercion). To contain such issues, it is recommended that personnel proceed on these kinds of activities in small groups.
    c. All assets must be inventoried (with a copy remaining with management in Canada) and, in higher threat areas, a destruction plan should be in place to ensure that the asset is rendered fully unusable and irreparable.
    d. Note also the direction above to ensure that all IT and telecommunications devices adhere to Agency-related guidance associated with encryption and other controls as determined by the IT Security and Information Security organizations.

*Response*

24. Ensuring a response capability is best established when in the preparation phase of such activities. The elements of response should ensure that the following are present:
    a. The response should be fully understood and must be approved by the employee`s management. The response should proceed, to the extent possible, through formal channels. While other forms of arrangement sometimes take place, it should be understood







that those arrangements may suffer diplomatic, legal or operational restrictions that can be overcome through diplomatic channels.

b. The response should be triggered by (1) a signal sent from the employee, (2) a signal sent from management or (3) from a trusted source such as the Mission Security Officer or local point of contact. It is important to understand that when such signals are received, the primary focus is ensuring that the employee is moved to a safe location before deciding to determine what the specific nature of the response should be.
c. The equipment used by the employee should take into account the reliability of the infrastructure in the area being visited. In areas where the infrastructure may be subject to disruption (for any number of reasons), consideration should be given to using technology that bypasses those vulnerabilities (such as satellite phones for remote areas without coverage).
d. Where the signal is sent, it should activate a plan that includes the notification of management, the nearest Canadian mission and other first response capabilities as determined on a case-by-case basis. Note that no communication is considered to be sent until a confirmatory message is received back.

25. The priority of response shall be the following:
    a. Upon receipt of the signal, the first step is movement to a safe location;
    b. Identifying the nature of the threat to the extent possible;
    c. Determining the status of the employee (health, how long safe, need to move, etc.);
    d. Activating any steps needed to contain events (preventing further injury or damage);
    e. Identifying the preferred next course of action (retrieval, relocation, embedding with mission);
    f. Identify the next time and method of communication.

26. The specific nature of the response will vary from situation to situation. It should be clear, however, that any trip of this extent should include the following:
    a. The ability to locate the employee without necessarily having to contact the employee (for higher risk environments),
    b. The ability to communicate, even if in a limited manner, in both directions to assist in maintaining clarity of the situation to the extent possible,
    c. Periodic reporting periods to be able to confirm that the employee is not in a position of risk or in need of assistance,
    d. A confirmation word (in addition to the *duress word*) that can be communicated to a third party by either the employee or management as a means of establishing that the third party does not pose a significant risk of inserting itself into the situation inappropriately or without the employee's or management's knowledge; and
    e. Response plans are to take into account steps that may be needed to protect the employee and also steps necessary, where warranted, to protect the family of the employee.







**Reporting Requirements**

*Routine Reporting*

27. Management and the employee should establish a routine reporting structure. These may be incorporated into normal reporting used for work. The purpose of this structure is to accomplish the following:
    a. Identify, through the absence or missing of a reporting cycle, the need to ascertain the status of the employee,
    b. Identify if lines of communication are available, and
    c. To afford the opportunity to communicate the *duress word* to covertly indicate that the employee is at risk.

*Security Incidents*

28. Security incidents are to be reported through the normal channels for reporting. These may vary from task to task.
    a. For international travel, the security incident should be reported to the nearest Canadian mission and to the Border Operations Center for purposes of immediate notification. If only one message can be sent without copies, then the primary message should include an instruction to forward the message to the other party.
    b. For remote travel, the notification that a security incident has taken place should be communicated to the point of contact established for the trip and as per Security Incident Reporting processes.

29. It should be noted that while the initial message may provide minimal information (i.e. advising of an incident involving a sensitive asset), a full report must be submitted to Security as per Security Incident Reporting processes at the first opportunity and as a priority report once the employee is able to do so.
    a. It is understood that it may take a period of time for the full report to be sent. The time limit to be used on this is that the report must be submitted to Security within 24 hours of the employee recommencing normal (assigned) operations.

*Personal Safety*

30. When reporting issues associated with personal safety, a series of reports are required. These are the following:
    a. Initial report: consisting of an extremely short and expedient message intended to simply alert the Agency for the need to assistance,
    b. Update reports: consisting of communications needed to maintain the response and ensure that the employee and sensitive assets (in order of priority) reach safety, and
    c. Full report: consisting of a detailed accounting of all actions, events and relevant information within 24 hours of returning to a safe location or to normal operations.







31. It is important that the initial call be made as quickly as possible. The reason for this is that it is unlikely that any response could be brought to play before it is known that the employee faces challenges. The initial notification, however, should be tailored to provide the following information (or as much as possible) without putting the employee at further risk:
    a. Name,
    b. Location,
    c. Nature of threat and likely impact,
    d. Immediacy (in terms of location and time).

*Roles and Responsibilities*

32. In general, senior management remains accountable under law and regulation regarding the taking of reasonable steps for the protection of persons performing work on behalf of the Agency.

33. The Departmental Security Officer is accountable, under the overall security and asset protection portfolio for the coordination of program and policy activities and is also delegated as the senior official within the Agency for decisions regarding security risk management.

34. The Manager, Physical Security is responsible for providing technical guidance, through the Director Infrastructure and Information Security, and advice to the Departmental Security Officer while also providing management supervision with respect to physical security services provided to the Agency.

**Supporting Material**

35. This standard falls under the Directive on Physical Security.

36. This standard should be read in conjunction with other Physical Security standards and guidance and is intended to describe certain specific steps unique to these environments.

**Enquiries**

37. Enquiries are to be forwarded to the Manager, Physical Security in HQ.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme en matière de sécurité matérielle dans les régions éloignées ou isolées

PROTECTION • SERVICE • INTÉGRITÉ





Cette norme entre en vigueur le 2 février 2015.

**Objectif**

1) Le présent document fournit des directives en ce qui concerne les activités associées à la conceptualisation, à la conception et à la mise en œuvre des contrôles de sécurité matérielle en tenant compte des régions à risque élevé, des régions isolées ou des endroits où une intervention efficace pourrait ne pas être possible. Le document comprend des exigences (indiquées à l'aide des termes « est tenu de » ou « doit ») et des recommandations (indiquées à l'aide des termes « devrait » ou « pourrait »).

**Intention**

2) L'intention du présent document est de fournir une orientation claire et concise concernant les diverses exigences en matière de sécurité matérielle aux personnes qui :
    a) voyagent dans des régions qui n'ont pas l'infrastructure ou les services nécessaires pour intervenir rapidement (en moins de 24 heures) lors d'événements liés à la sécurité ou d'enjeux liés à la sécurité personnelle ;
    b) voyagent à des endroits qui présentent une probabilité modérée ou élevée d'avoir d'importants événements pouvant engendrer la destruction de l'infrastructure ou la perturbation des services, ce qui rendrait une intervention plus difficile ;
    c) voyagent à des endroits où le niveau de confiance envers les premiers intervenants pourrait être remis en question, ce qui pourrait rendre une personne encore plus à risque.
    d) Il faut comprendre que ces milieux de travail peuvent se trouver au Canada (bureaux d'entrée isolés ou environs) ou à l'étranger (pays où la présence canadienne est limitée). Ces événements peuvent également découler de catastrophes naturelles (au Canada ou à l'étranger) qui détruisent l'infrastructure ou perturbent les services nécessaires à une intervention efficace. Les directives fournies dans le présent document doivent être lu en tenant compte des circonstances particulières dans lesquelles se trouve ou pourrait se trouver le personnel.

3) Il faut lire le présent document en se référant aux autres normes et directives de la Sécurité matérielle. Il a pour but de fournir des directives particulières puisque conformément à ces normes, on suppose que les services et l'infrastructure nécessaires à une intervention sont fiables et se trouvent dans la région. Lorsque vous consultez les autres normes, leur intention doit être prise en considération en fonction de l'objectif de sécurité à atteindre.

**Portée**



4) La norme concerne toutes les activités de l'Agence pour lesquelles il faut prendre des mesures raisonnables pour protéger le personnel, les biens de nature délicate (y compris les renseignements) ou les activités.

**Exigences**

*Générales*

5) Les personnes qui planifient des activités doivent tenir compte de la capacité à intervenir lors de différentes menaces à la sécurité matérielle. Avant d'entreprendre un tel voyage, la direction responsable doit avoir effectué une évaluation afin de déterminer quels sont les risques relatifs à la sécurité matérielle pour les biens et l'information et les risques en matière de sécurité personnelle.

6) Lorsqu'elle effectue ces évaluations, la direction doit tenir compte du contexte de la menace et du type de menace susceptible de faire surface dans le contexte opérationnel :
   a) Il faut s'assurer que les plans d'évacuation ou de rapatriement d'une personne ou des biens de nature délicate mis en place pour des activités ayant lieu dans une localité qui fait l'objet d'un avis au voyageur (avis officiels comme ceux du Ministère des Affaires étrangères, du Commerce et du Développement, du Bureau des affaires consulaires des États-Unis ou d'une source officielle semblable) ou qui s'avère dans un environnement à risque ÉLEVÉ tiennent compte de la possibilité de ne plus compter sur l'infrastructure ou les services provenant de l'extérieur de l'Agence ;
   b) Il faut tenir compte de la capacité d'assurer la communication avec les personnes sur place et mettre en place des plans permettant le rapatriement du personnel et des biens de nature délicate dans le cas d'activités ayant lieu dans une localité difficile d'accès (y compris dans des situations de sauvetage) et où la communication est difficile ou soupçonnée de l'être.

7) Dans ce type d'activités, l'accent est mis sur la préparation, la prévention, la maîtrise et l'intervention, lesquelles sont définies ci-dessous.
   a) **Préparation** – préparation personnelle, de l'obligation d'informer la personne des risques auxquelles elle pourrait faire face et à la formation qui lui serait utile pour atténuer ces risques (comme la formation relative aux milieux hostiles, la formation en techniques de survie et les techniques de protection rapprochée) ;
   b) **Prévention** – contrôles physiques, procéduraux, techniques ou administratifs dont le but est de faire en sorte que la personne, le bien ou l'activité est protégé dans la mesure du possible ;
   c) **Maîtrise** – mesures immédiates à prendre lorsqu'on estime qu'une personne ou un bien de nature délicate est exposé à un niveau de risque inacceptable ;







d) **Intervention** – mesures coordonnées et gérées prises afin de passer de la maîtrise à la reprise éventuelle des activités ; et

e) *La principale différence entre la maîtrise et l'intervention est que la maîtrise est décrite en termes d'objectifs à atteindre et est sous la responsabilité immédiate de l'agent sur place, alors que l'intervention est une activité gérée qui suit certaines étapes prédéterminées pour effectuer des tâches ou atteindre les objectifs susmentionnés. Par exemple, lorsqu'un agent découvre une bombe près d'une voiture, à l'étape de la maîtrise il s'éloignera du lieu rapidement (maîtrisant ainsi le risque de blessures personnelles) et communiquera avec la personne-ressource appropriée en vue d'informer la direction de la situation. À l'étape de l'intervention, la direction déplacera les activités à un emplacement secondaire ou cessera temporairement les activités, selon la situation.*

8) Lorsqu'on envisage de déployer une personne pour des activités dans de telles circonstances (dans les régions éloignées ou isolées), il faut évaluer cette dernière en fonction des critères suivants. Fait à noter, cette méthode d'évaluation n'est pas utilisée pour évaluer le rendement ou la capacité de travailler de la personne, mais plutôt pour aider l'Agence dans le processus d'évaluation des risques relatifs à la sécurité matérielle :

   a) **Cibles renforcées** – les personnes qui connaissent les risques, ont reçu une formation pour faire face aux menaces les plus probables dans la région (comme une catastrophe naturelle), ont pris les mesures nécessaires pour atténuer ces risques (comme les vaccins) et sont en mesure de continuer leurs activités pour un maximum de 96 heures. Les cibles renforcées ont probablement une formation et de l'expérience de travail dans des environnements difficiles ou complexes.

   b) **Cibles modérées** – les personnes qui connaissent les risques, sont familières avec les techniques courantes pour traiter ces risques et sont en mesure de continuer leurs activités pour un maximum de 48 heures. Les cibles modérées peuvent avoir une formation limitée ou de l'expérience de travail à l'étranger, mais pas dans des environnements difficiles ou complexes.

   c) **Cibles vulnérables** – les personnes qui connaissent les risques, sont familières avec les techniques utilisées, mais n'ont pas de formation complète sur la façon de faire face aux risques les plus probables dans la région et auraient besoin d'aide pour continuer leurs activités pour un maximum de 48 heures. Les cibles vulnérables n'ont probablement pas de formation ou d'expérience de travail à l'étranger ou dans des pays autres que les pays amis du Canada.

**Méthodologie et directives particulières**

*Préparation*

*Évaluation des risques*



9) Pendant la préparation de ce type d'activités, il faut tenir compte des risques raisonnablement prévisibles et déployer des efforts raisonnables pour prendre connaissance des points suivants :
   a) **Menaces intentionnelles** – celles mentionnées dans les séances d'information du SCRS et des organismes d'exécution de la loi ainsi que tout autre renseignement concernant les menaces liées au terrorisme, le crime organisé, les crimes locaux et la corruption,
   b) **Menaces accidentelles** – celles mentionnées dans les sources ouvertes (communiquer avec la Section de la sécurité matérielle), y compris les avertissements liés aux accidents de la route, aux normes de construction (ou absence de norme) et les coutumes locales qui pourraient engendrer des conflits,
   c) **Menaces naturelles** – celles mentionnées dans diverses bases de données de gestion des urgences, par les services météorologiques, par l'Organisation mondiale de la santé et les organisations de voyage (particulièrement en matière de faune et de flore).
10) Même si l'Agence procède à une évaluation des risques, la personne déployée doit rester vigilante et consulter les avis aux voyageurs et autres sources d'information officielle jusqu'au point de départ.
11) Dans tous les cas, on recommande de préparer un itinéraire avec des points d'appel (au point de départ, à l'arrivée dans la ville, après le dédouanement, au départ vers la localité et à l'arrivée à la localité) et un plan détaillé des heures d'arrivée à chaque point. Dans les régions où le risque est élevé, le plan devrait inclure les situations où la personne manque le point d'arrivée préétabli. Dans les cas où la menace est élevée, l'itinéraire devrait également inclure *un signal de contrainte* qui peut servir à informer discrètement une personne que l'agent a besoin d'aide, mais ne peut le demander ouvertement. Il faudrait déterminer les directives à suivre durant les périodes où la communication n'est pas possible.

*Recommandation pour une formation spécialisée*

12) Lorsqu'on estime que la sécurité d'une personne est à risque, il faut prendre les mesures nécessaires pour s'assurer que la personne suit la formation appropriée :
   a) dans les cas de **conflit**, la personne devrait suivre la *formation relative aux milieux hostiles* ou une formation semblable en protection personnelle selon l'organisme gouvernemental (MDN pour les conflits, SCRS pour la sécurité personnelle, etc.) ;
   b) dans les cas de **catastrophe naturelle ou de conditions difficiles**, la personne devrait suivre une formation de base sur les techniques de survie et une formation avancée en secourisme ;
   c) dans les cas où il y a risque de maladie ou de contagion, la personne devrait assister à une séance d'information offerte par un représentant de l'Organisation mondiale de la Santé en ce qui concerne les étapes à suivre pour atténuer les risques ;
   d) fait à noter, les discussions sont entamées à propos des formations susmentionnées afin d'assurer leur disponibilité.

*Limiter l'exposition des biens de nature délicate*







13) Lorsqu'on envisage un tel voyage, il faut tenter de limiter l'exposition des biens de nature délicate. Il faut assurer l'équilibre entre le besoin des biens aux fins opérationnelles, la présence de la personne sur le terrain et la possibilité d'exposer les biens à des risques.
    a) Dans le cas des **appareils de télécommunication**, la personne doit tenir compte des directives du Centre de la sécurité des télécommunications Canada (CSTC) en matière de protection des appareils de communication mobiles et des ordinateurs portables.
    b) Lorsqu'il est question de **biens contrôlés**, le numéro de série du bien doit être envoyé au gestionnaire responsable du programme et au coordonnateur national des biens de sécurité contrôlés (s'il s'agit d'un bien de sécurité contrôlé). La sécurité régionale devrait être aussi informée.
        i) *À l'extérieur du Canada* – Il faut comprendre, cependant, qu'à moins que l'Agence ait directement et spécifiquement autorisé l'utilisation d'un bien contrôlé à l'étranger, ce dernier doit rester au Canada. Les biens de sécurité contrôlés ne devraient être déplacés, dans la mesure du possible, que dans des sacs diplomatiques.
        ii) *Au Canada* – les biens contrôlés, à l'exception des pièces d'identité et les insignes, devraient rester demeurer au bureau d'entrée assigné (par exemple, les timbres de port, armement).
    c) Lorsqu'on propose des **installations**, la planification du projet devrait être faite par des organisations qui comprennent le milieu ciblé :
        i) *Dans le cas d'un voyage à l'étranger*, il s'agit de la mission canadienne la plus près avec une description claire de tous les travaux potentiels à faire.
        ii) *Dans le cas d'un voyage à l'intérieur du pays*, il s'agit des entités de confiance et des coordonnateurs de voyage qui ont une connaissance directe du lieu et de son environnement. Idéalement, il faudrait communiquer avec le personnel local (ou au moins les personnes qui connaissent bien l'environnement local) pour déterminer ce qui doit être pris en considération.
    d) Lorsqu'on fait des **préparatifs à long terme**, il faut identifier des sources de nourriture et d'eau fiables provenant de missions locales.
    e) *On recommande fortement qu'avant le départ, la direction effectue une évaluation de tous les biens de l'Agence proposés pour le déplacement vers un environnement étranger en vue de déterminer (1) si le bien est vraiment requis et (2) jusqu'à quel point les processus ou les méthodes de l'Agence seront compromis (en raison de pratiques comme la rétro-ingénierie) si les outils échappent au contrôle de l'Agence.*
    f) *On recommande fortement à la direction de confirmer toutes les ententes faites avec les nations alliées pouvant servir lorsqu'un agent doit être retiré d'une région qui représente un risque grave et immédiat. Fait à noter, il faut faire preuve de prudence lors des discussions si ces nations affichent des positions concurrentielles.*

*Restriction de l'accès aux renseignements personnels et copie de sauvegarde des renseignements personnels*







14) On recommande fortement aux personnes de prendre les mesures nécessaires pour protéger leurs renseignements personnels et restreint leur accès à l'étranger. Ces mesures peuvent comprendre un plan d'urgence qui inclut le téléchargement d'une page numérisé du passeport, du visa, et du carnet de vaccination sur un nuage informatique sécurisé (protégé par deux mots de passe). Bien que cette mesure puisse sembler illogique, l'objectif est d'atténuer le risque lié avec l'établissement de l'identité d'une personne si elle perd ses documents.

15) On recommande fortement aux personnes d'obtenir un bracelet d'identification MedicAlert ou un produit semblable identifiant leurs allergies, et autres conditions, puisque les dossiers médicaux pourraient ne pas être disponibles. L'information doit également être fournie à la direction (pour les voyages nationaux et internationaux) et à la mission canadienne la plus près (pour les voyages à l'étranger).

16) On recommande fortement à la personne de faire en sorte que toutes ses coordonnées sont à jour (coordonnées au travail, personnes-ressources en cas d'urgence au travail et personnes-ressources en cas d'urgence familiale) et que tous ses documents juridiques (assurances, etc.) sont à portée de la main avant de partir.
    a) Une des principales sources de stress ou de distraction durant ces affectations est les problèmes familiaux qui perdurent. Puisque ces distractions peuvent engendrer un manque de souci du détail rendant la personne vulnérable dans un endroit peu familier, on recommande fortement que les préparatifs au voyage comprennent de s'assurer que les questions financières et scolaires sont réglées et que toute autre obligation familiale soit traitée, dans la mesure du possible;
    b) On recommande de s'assurer que la famille connaisse les moyens de communication et les services offerts par la mission canadienne.

*Trousse de voyage*

17) On recommande aux personnes de voyager avec une trousse de voyage qu'elles peuvent porter en tout temps. La trousse devrait contenir les informations suivantes dans le cas d'activités à l'étranger :
    a) Une copie de tous les documents essentiels (passeport, visa, carnet de vaccination, autorisations) dans un sac étanche ;
    b) Une copie de toute prescription (en s'assurant qu'elle soit clairement lisible) et assez de médicaments pour couvrir une période d'au moins 72 heures ;
    c) Les coordonnées des personnes-ressources en cas d'urgence (il devrait s'agir des coordonnées de la mission canadienne la plus près ou la ligne d'accès direct des voyageurs du MAECD. Pour obtenir ces coordonnées, veuillez consulter le site Web du MAECD : http://voyage.gc.ca/assistance/assistance-d-urgence ;
    d) Des comprimés pour purifier l'eau ;



e) Assez de barres à haute valeur énergique pour 48 heures si elles peuvent être transportées légalement (si ce n'est pas le cas, achetez des barres dans des emballages scellés après le dédouanement) ;
f) Des marqueurs et du papier hydrofuge ; et
g) Des vêtements appropriés pour le climat.

18) On recommande aux personnes qui travailleront dans des régions éloignées de prendre les mesures nécessaires pour avoir assez de chaleur, d'eau, de nourriture et un abri pour au moins 72 à 96 heures. Il faudrait aussi considérer le recours à d'autres ressources pour maintenir la communication sans avoir à dépendre des infrastructures terrestres, particulièrement dans les régions où l'accès au cellulaire ou à des méthodes de communication semblable est faible ou nul.

19) On recommande aux personnes de conserver une petite somme d'argent à deux endroits sur leur corps pour avoir une réserve liquide. Il est important de comprendre que les systèmes de transaction bancaire électronique d'un grand nombre de pays ne respectent pas les mêmes normes que ceux en Amérique du Nord.
   a) Dans certains pays, il peut être nécessaire d'avoir une carte de débit prépayée (qui n'est pas liée à un compte bancaire) ayant une somme d'argent suffisante pour faire des transactions afin de limiter le recours aux comptes bancaires personnels et éviter ainsi qu'ils soient compromis.

*Planification de l'itinéraire*

20) Le personnel en transit fait souvent l'objet d'une série de menaces allant de la menace hostile intentionnelle à la menace naturelle. C'est pourquoi les personnes qui travaillent dans une région éloignée ou isolée doivent tenir compte des directives suivantes lorsqu'elles planifient l'itinéraire :
   a) toujours avoir un itinéraire et en envoyer une copie au point de contact à destination et, si possible, à la direction. Au moins deux parties de confiance devraient toujours être au courant de votre emplacement et de vos activités ;
   b) dans les zones à risque élevé, restez à l'affut des secteurs où le taux de criminalité est plus élevé et de ceux qui font l'objet de perturbations causées par des manifestations, des catastrophes naturelles ou des événements particuliers ;
   c) dans les zones à risque élevé, variez vos itinéraires, les heures de départ et, si possible, les véhicules utilisés afin de déjouer les personnes tenteraient de déterminer vos comportements à des fins de planification ;
   d) en chemin, établissez des points de rupture que vous pourrez utiliser pour rapidement contourner des obstacles ou événements perturbateurs. Si vous voyagez sur des routes isolées, soyez au courant des sorties, des voies de détresse et de ce type de routes ;
   e) évitez les secteurs où il y a de la congestion ou du trafic puisqu'ils peuvent encourager les activités criminelles (de la piraterie routière au cambriolage avec effraction). Il faut



également connaître les secteurs qui font l'objet de restrictions en raison des conditions climatiques ;

f) toujours laisser votre véhicule dans un endroit sécuritaire ou sous la surveillance d'une entité digne de confiance (coordonnée ou approuvée par la mission canadienne dans la région). Avant de partir, assurez-vous de vérifier le véhicule, la condition des pneus, les passages de roue ou tout signe de fuite sous la voiture ;
g) à la fin de chaque déplacement, vérifiez le niveau de carburant et d'autres fluides du véhicule pour vous assurer qu'il est prêt pour son prochain voyage ;
h) si vous louez une voiture, ne la réservez pas en avance et changez de véhicule régulièrement ;
i) ne laissez jamais d'information ou de biens de nature délicate dans le véhicule à moins que ce soit dans une boîte verrouillée et fixée, au besoin, dans le coffre de la voiture. Les biens de l'Agence ne doivent pas être exposés et laissés sans surveillance sur les sièges, entre les sièges ou dans un endroit bien en vue.

*Prévention*

21) La clé de la prévention est, d'une part, de faire en sorte que les employés restent à l'affut et demeurent vigilants et, d'autre part, que tous les préparatifs soient effectués par l'entremise de parties de confiance (mission).

22) Lorsque vous envisagez des mesures préventives, il faut tenir compte de ce qui suit :
   a) faire en sorte que les personnes qui voyagent sont accueillies aux douanes par une personne de la partie opposée et que la rencontre soit coordonnée à l'aide de voies fiables mutuelles ;
   b) utiliser uniquement les véhicules fournis par la mission ;
   c) utiliser uniquement les appareils de communication fournis par l'Agence pour les communications officielles et conformément aux directives de la Sécurité de l'information et de la sécurité des TI ;
   d) faire en sorte que tous les objets de valeur personnels sont en lieu sûr, à la maison ou dans les locaux de la mission et non sur votre personne ;
   e) utiliser uniquement des dispositifs de stockage amovibles dont la méthode de chiffrement a été approuvée par l'Agence, conformément aux directives de la Sécurité de l'information et de la sécurité des T I;
      i) dans les zones de risque élevé où ce type de dispositif est essentiel, on recommande fortement que les données contenues sur le dispositif puissent être effacées à distance en cas de perte ou de vol ;
   f) faire en sorte que les vêtements et autres accessoires similaires conviennent au climat et puissent aider à prévenir l'exposition à diverses formes de maladies ou de contamination. Tenir compte de la possibilité et la probabilité de changements climatiques, y compris des conditions météorologiques extrêmement défavorables, selon la région ;







g) prévoir du temps pour permettre aux vaccins ou autres mesures médicales d'agir ;
h) *Veuillez noter que dans les environnements où il existe un important aspect de compétition par rapport aux opérations (à des fins commerciales par exemple), il est possible qu'une personne souhaitant tirer avantage de la situation entre dans votre chambre d'hôtel ou autre type d'hébergement semblable. Dans ce cas, il ne faut pas considérer que les valises verrouillées ou une affiche « ne pas déranger » seront des mesures de dissuasion suffisantes.*

*Maîtrise*

23) Comme il a été susmentionné, la maîtrise fait référence aux étapes prises immédiatement après un incident, en réaction quasi instinctive. Ces mesures ne font pas partie de l'intervention. Elles ont pour objectif de faire en sorte que la personne est en mesure de reprendre le contrôle de la situation, l'évaluer et entamer l'intervention appropriée.
   a) Pour les employés, l'objectif est de détecter les événements suspects ou potentiellement hostiles. Dans un tel cas, la priorité est de vous déplacer dans un endroit sécuritaire. Il faut désigner des endroits sécuritaires le long des routes fréquentées ou près des aires de travail où vous pourrez vous déplacer rapidement et sans trop de difficulté.
   b) Le personnel doit comprendre que les employés ou représentants de l'Agence sont surveillés par diverses entités. Bien qu'il soit possible de vivre la culture et les traditions locales et de tirer parti de l'expérience, on recommande de s'adonner à ces activités avec modération et de les planifier de façon à ne pas laisser la personne vulnérable à différentes menaces (que ce soit un enlèvement, une activité criminelle, un cas de harcèlement sexuel, ou une autre forme d'extorsion / de coercition). Afin d'éviter ces situations, on recommande au personnel d'effectuer ces activités en petits groupes.
   c) Tous les biens doivent être répertoriés (une copie doit être entre les mains de la direction au Canada) et, dans les zones à risque élevé, un plan de destruction doit être en place pour s'assurer que le bien en question ne peut plus servir ou être réparé.
   d) Comme il a été susmentionné, il faut faire en sorte que tous les appareils de la TI et les dispositifs de télécommunication respectent les méthodes de chiffrement et autres contrôles approuvés par l'Agence, conformément aux directives de la Sécurité de l'information et de la sécurité des TI.

*Intervention*

24) C'est à l'étape de la préparation de l'activité qu'il faut établir la capacité d'intervention. L'intervention devrait tenir compte des éléments suivants :
   a) La direction du personnel doit entièrement comprendre et approuver l'intervention. L'intervention devrait être effectuée, dans la mesure du possible, à l'aide de voies officielles. Bien que d'autres dispositions soient prises parfois, il faut comprendre qu'elles pourraient faire l'objet de restrictions diplomatiques, juridiques ou opérationnelles pouvant être allégées grâce aux voies diplomatiques.







b) L'intervention devrait être déclenchée par (1) un signal envoyé par l'employé, (2) un signal envoyé par la direction ou (3) une source fiable comme l'agent de sécurité de la mission ou un point de contact local. Il faut comprendre que dès la réception d'un tel signal, l'objectif premier est de s'assurer que l'employé est en lieu sûr avant de décider la nature exacte de la réponse.

c) L'équipement utilisé par l'employé doit tenir compte de la fiabilité de l'infrastructure de la région. Dans les secteurs où l'infrastructure pourrait être exposée à des perturbations (pour de nombreuses raisons), il faudrait étudier la possibilité de recourir à une technologie qui évite ces vulnérabilités (comme les téléphones satellites pour les régions éloignées sans couverture).

d) Lorsque le signal est envoyé, il devrait déclencher un plan qui comprend l'envoi d'un avis à la direction, à la mission canadienne la plus près et aux autres services de première intervention, déterminé au cas par cas. Veuillez noter que pour considérer un message comme étant envoyé, il faut d'abord avoir reçu un avis de confirmation.

25) La priorité des étapes de l'intervention est établie comme suit :

a) envoyer l'employé en lieu sûr, dès la réception du signal ;
b) identifier la nature de la menace dans la mesure du possible ;
c) déterminer le statut de l'employé (santé, en sécurité pour combien de temps, besoin de le déplacer, etc.) ;
d) entamer toute mesure nécessaire pour maîtriser l'événement (éviter toute autre blessure ou tout autre dommage) ;
e) déterminer les mesures préférables à prendre (rapatriement, déménagement, intégration à la mission) ;
f) déterminer la méthode de communication et le moment où le prochain message sera envoyé.

26) La nature particulière de l'intervention varie d'une situation à l'autre. Toutefois, il faut préciser que tout voyage de cette ampleur doit tenir compte des éléments suivants :

a) la capacité de localiser l'employé sans avoir à communiquer avec lui directement (dans les zones à risque élevé) ;
b) la capacité de communiquer bilatéralement, même de façon limitée, pour aider à clarifier la situation dans la mesure du possible ;
c) des rapports périodiques en vue de confirmer que l'employé n'est pas en danger ou qu'il n'a pas besoin d'aide ;
d) un signal de confirmation (autre que le *signal de contrainte*) que l'employé ou la direction peut communiquer à une tierce partie afin d'établir que cette dernière ne représente pas une importante menace si elle s'immisce dans la situation sans prévenir l'employé ou la direction ;
e) un plan d'intervention qui tient compte des mesures à prendre pour protéger les employés et, au besoin, leur famille.





**Exigences en matière de rapport**

*Rapport sur les activités de routine*

27) La direction et l'employé devraient établir une structure de rapport pouvant être incluse aux rapports déjà soumis régulièrement pour le travail. L'objectif de la structure est d'accomplir ce qui suit :
   a) déterminer, en raison de l'absence d'un cycle de rapports, qu'il faut vérifier le statut de l'employé;
   b) déterminer si les voies de communication sont disponibles;
   c) donner l'occasion de communiquer le *signal de contrainte* pour indiquer discrètement que l'employé est en danger.

*Incidents de sécurité*

28) Les incidents de sécurité doivent être signalés à l'aide des voies normales d'établissement des rapports, lesquelles peuvent varier d'une tâche à l'autre.
   a) Pour un voyage international, l'incident de sécurité doit être signalé à la mission canadienne la plus près et au Centre des opérations frontalières pour avis immédiat. Si un seul message peut être envoyé, sans copie, il doit contenir une directive pour le transférer à l'autre partie.
   b) Pour un voyage en région éloignée, l'incident de sécurité doit être signalé au point de contact établi pour le voyage, conformément au processus d'établissement des rapports d'incidents de sécurité.

29) Fait à noter, bien qu'il envoie un message initial contenant les informations essentielles (c.-à-d. signalant un incident qui implique un bien de nature délicate), l'employé doit tout de même soumettre un rapport complet prioritaire à la Sécurité le plus tôt possible.
   a) Il est évident que l'envoi d'un rapport complet peut prendre un certain temps. La règle générale à utiliser est que le rapport complet devrait être soumis à la Sécurité dans les 24 heures suivant la reprise des activités normales de l'employé.

*Sécurité personnelle*

30) Lorsqu'il est question de rendre compte des enjeux associés à la sécurité personnelle, certains rapports sont nécessaires :
   a) Rapport initial : un message très court et direct dont le but est simplement d'avertir l'Agence que l'employé a besoin d'aide ;
   b) Rapport de mise à jour : communications nécessaires pour assurer l'intervention et faire en sorte que l'employé et les biens de nature délicate (selon l'ordre de priorité) sont en sécurité ;
   c) Rapport complet : compte rendu détaillé de toutes les mesures prises, les événements et les informations pertinentes envoyé dans les 24 heures suivant l'arrivée en lieu sûr ou le retour aux activités régulières.



31) Il est important que l'appel initial soit fait le plus rapidement possible puisqu'il est peu probable qu'une intervention soit entamée avant de savoir que l'employé fait face à une situation difficile. L'avis initial, toutefois, doit fournir les informations suivantes (dans la mesure du possible) sans créer un risque supplémentaire pour l'employé :
   a) Nom
   b) Lieu
   c) Nature de la menace et répercussions probables
   d) Imminence (en matière de lieu et de temps)

*Rôles et responsabilités*

32) En général, la haute direction est tenue, conformément aux lois et règlements, de prendre les mesures raisonnables pour assurer la protection des personnes qui travaillent au nom de l'Agence.

33) L'agent de sécurité du ministère est tenu, conformément à l'ensemble du portefeuille de sécurité et de protection des biens, de coordonner les activités de programme et les activités stratégiques, en plus d'être délégué à titre de cadre supérieur à l'Agence pour prendre des décisions concernant la gestion des risques pour la sécurité.

34) Le gestionnaire de la Sécurité matérielle est tenu de fournir des directives, par l'entremise du directeur de l'Infrastructure et la Sécurité de l'information et de conseiller l'agent de sécurité du ministère tout en supervisant les services de sécurité matérielle fournis à l'Agence.

**Documents à l'appui**

35) La norme relève de la Directive sur la sécurité matérielle.

36) Il faut lire le présent document en se référant aux autres normes et directives de la Sécurité matérielle, puisqu'il décrit certaines étapes uniques à ces milieux de travail.

**Questions**

37) Vous pouvez envoyer vos questions au gestionnaire de la Sécurité matérielle.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for Security Incident Reporting

PROTECTION • SERVICE • INTEGRITY

Canada



This Standard takes effect on February 2, 2015.

**Purpose**

1) The purpose of this standard is to provide the Canada Border Services Agency (CBSA) with a structured approach to ensure the implementation and establishment of effective reporting of security incidents.

**Intent**

2) The intent of this document is to define the proper reporting of Security Incidents. Security incidents, when reported in a complete and timely manner, are an important part of the Agency's ability to contain, mitigate, address and otherwise respond to acts or conditions that may pose a range of risks to Agency personnel, assets, information, and operations and to carry out the necessary measures against these risks.

**Application**

3) The Standard on Security Incident Reporting is applicable to all persons, regardless of their employment status, and applies to any CBSA operation or sensitive asset , including those entrusted to us by a third party.
4) Note that this standard does not include any requirements for Border Operations Centre (BOC), Occupational Health and Safety (OHS) or other program reporting. For guidance specific to those reporting requirements, contact the management responsible for those programs.

**Category of Incidents**

5) Security incidents encompass any and all of the following:
   ***a)*** ***Threats -*** in terms of any act or condition that could pose a risk of loss (including unauthorized disclosure, disruption and injury) to CBSA personnel, assets, information, or operations. These are considered separate from security incidents and breaches in that the threat has not yet taken any action against the Agency, its personnel or its operations.
   b) ***Violations*** – in terms of any act or condition (intentional or otherwise) which results in a security control being bypassed, defeated or otherwise reduced in its ability to meet management`s expectation with respect to the management of physical security risk.
   c) ***Incidents*** – events or discovered conditions that involve a threat exploiting a vulnerability but for which there is no indication that an injury (in terms of disclosure, disruption, modification, loss or injury) has occurred.



d) ***Breaches*** – events or discovered conditions that involve a threat having apparently exploited a vulnerability (or equivalent) but for which there is **a defined and measurable loss** or injury.

6) There are four categories of incidents. These are the following:
   a) ***Critical Incidents*** – these are defined as those incidents which have resulted in an injury to personnel. This is based on the definition used by the Critical Incident Management Working Group (CIMWG) and not be confused with issues associated with Critical Infrastructure or vital services.
   b) ***High Priority*** – these are defined as those incidents that have impacted **VERY HIGH** or **HIGH** value assets (as described in the Harmonized Threat and Risk Assessment methodology put forward by the RCMP and CSEC in Tables B-2 and B-3 (pages B-7 and B-8 of the standard which can be found at http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf ))
   c) ***Medium Priority*** – these are defined as those incidents that have impacted MEDIUM to LOW value assets (as described in the Harmonized Threat and Risk Assessment methodology put forward by the RCMP and CSEC in Tables B-2 and B-3 (pages B-7 and B-8 of the standard which can be found at http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf )) They also include *threats* that may pose a risk (not immediate) in terms of injury to personnel or the potential to cause losses to HIGH value assets,
   d) ***Administrative*** – these are defined as those incidents that have impacted VERY LOW value assets.

   Note that where ID Cards or other tokens granting access are involved, the level of access is to be used in terms of determining whether or not the incident is to be considered a LOW or MEDIUM priority. For example, an ID card that grants access to an area where Protected B information is processed, a MEDIUM value would be assigned (based on the RCMP standard) whereas one that opens locks to a SECRET processing area would be considered a HIGH value.

**Reporting Requirements**

7) A Security Incident Report (SIR) is to be submitted using the approved CBSA form (BSF 152). In circumstances that this may not be possible, the focus is to be on providing full and complete information.

8) All incidents must be reported in a complete and timely manner in order to ensure the Agency's ability to contain, mitigate, address and otherwise respond to acts or conditions that may pose a range of risks to Agency personnel, assets (including information), and operations.

9) **Critical incident** and **HIGH** value reporting requirements are as follows (note the definition used is the definition put forward by the CIMWG):
   - The Initial notification of the incident must be sent via encrypted (PKI) e-mail to the general Security Incident Report (SIR) Mailbox (Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca) with a copy to the Regional Security Manager







(RSM) or Headquarters Security Manager (HQSM) with ``High Importance“ . If it is being reported to the Border Operations Center (BOC), the requirements can be met by ensuring that the SIR mailbox is copied on the e-mail;

- The completed SIR is required to be received within 24 hours of resumption of normal operations to the general SIR mailbox with a copy to the Regional Security Manager (RSM) or Headquarters Security Manager (HQSM) . Where the BOC is being kept informed of events as they occur, this requirement can be met by copying the SIR mailbox. The completed SIR must contain a full synopsis of the event, its consequences, its root causes and follow up activities (including corrective measures).

  Note: There is the potential for follow up questions through the Regional or Headquarters Security Manager, or the Departmental Security Officer.

  Note: The HQSM plays the same role as the RSM, however in HQ. The HQSM is not to be confused with HQ security reporting Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca

10) **High** priority incidents (where the BOC is not notified) are to be reported as follows:
   - The Initial notification of the incident must be sent via encrypted (PKI) e-mail to the general SIR Mailbox (Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca) with a copy to the RSM or HQSM.
   - The completed SIR must be sent to the general SIR mailbox within 24 hours of resumption of normal operations with a copy sent to Regional or HQ Security.
   - The completed SIR must contain a full synopsis of the event, its consequences, its root causes and follow up activities (including corrective measures).

   Note: Those submitting the SIR should be aware of the potential for follow-up questions through the Regional or Headquarters Security Manager, or the Departmental Security Officer.

11) **Medium Priority** are to be reported as follows:
   - The Initial notification of the incident must be sent via encrypted (PKI) e-mail to the general SIR (Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca) with a copy to the RSM or HQSM within 24 hours of the initial incident;
   - The completed Security Incident Report (SIR) is required to be received within 96 hours of the resumption of normal operations or, if operations were not disrupted, within 96 hours of the sending of the initial report.
   - The completed SIR must contain a full synopsis of the event, its consequences, its root causes and follow on activities (including applicable corrective measures).

Note: Those submitting the SIR should be aware of the potential for follow on questions through the Regional or Headquarters Security Manager.

12) **Administrative** incidents are to be reported as follows:
- The completed SIR must be sent to either the Regional or Headquarters Security Manager with a cc to the Security Incident Reporting mailbox within one week of the initial incident.
- The completed SIR must contain a full synopsis of the event, its consequences, its root causes and follow on activities (including applicable corrective measures).

Note: Those submitting the SIR should be aware of the potential for follow-up questions through the RSM or HQSM.

13) General Information to be Included
- "Who, what, when, where and how" pertinent to the incident,
- Identification of the asset (serial number, unique identifying number),
- Any costs involved (cost of replacement, interim solution), if applicable,
- The nature and duration of any disruption, if present,
- Any corrective actions taken or mitigating measures put in place, and
- File numbers for police reports (if applicable), CPIC, etc. that may be relevant in an investigation.

**Duplication of Reports**

14) Where a formal report has been submitted to another part of the Agency that covers the information above, a copy of that report may be submitted and considered to have met the SIR reporting requirement. A follow up from Regional or HQ Security should be expected to ensure that there are no gaps in information.

**Roles and Responsibilities**

15) Department Security Officer (DSO)

The DSO is responsible for the overall Security program within the CBSA.

16) Director, Infrastructure and Information Security Division (IISD)

The Director is accountable for the implementation, strategic management and oversight of the Physical Security Program for the Agency and ensuring that the priorities of the program remain aligned with those of the Agency.

17) Manager, Physical Security Section (PSS)



The Manager of PSS is responsible for the operational management of the physical security program which includes:

- Developing processes and strategies for the mitigation of security incidents;
- Developing, implementing and communicating the standard to be used for Security Incident Reporting. This includes being able to formally request information under the authority of the DSO in order to determine the scope and impact of a security incident;
- Acting as the functional authority with respect to physical security impact analysis within the Agency;
- Ensuring continuity and consistent application across CBSA; and
- Ensuring compliance nationally.

18) Security Incident Coordinator, PSS

The Security Incident Coordinator (PSS) is responsible for:

- Conducting preliminary assessment, analyses and validates all incoming security incidents;
- Performing quality assurance monitoring to ensure integrity and quality of information;
- Conducting follow-up activities on security incidents by initiating a tracking system, consulting with HQ and regional clients, verifying all new data, updating the security database, and preparing supplementary reports if required;
- Conducting impact analysis and trend identification; developing preliminary conclusions and presenting these to the Manager PSS for future investigation and assessment; and
- Providing guidance and assistance to senior management, clients and regional offices regarding data collection methods, validating data, identifying and seeking clarification on inconsistencies, and consolidating data for the preparation of various reports.

*Regional Security Manager (RSM) and Headquarters Security Manager (HQSM)*

19) The RSM and HQSM are the delegated authority by the DSO for delivery of the physical security program, who act on behalf of the Manager of PSS within the Regions and HQ. The RSM or HQSM:

- Ensures the completeness of all security incident reports;
- Analyzes, assesses and validates incoming information while ensuring proper follow-up for missing information to PSS;
- Provides recommendations for corrective measures when required;
- Ensures compliance with all related Physical Security directives, policies, standards, guidelines and procedures within their Region or PSS;
- Aids in the completion of audits, reconciliations and requests initiated by the PSS; and,



- Ensures regional awareness and training related to security incidents.

**Consequences**

20) The timely reporting of security incidents is a significant part of ensuring that the physical security program is aware of and can focus on issues relevant to the Agency. Failure to take reasonable steps to report a security incident may result in administrative, civil or criminal prosecution depending upon the nature of the incident and the findings of any follow-up investigation.

**Supporting Material**

21) This standard falls under the Directive on Physical Security and operates in conjunction with the following:
    a. Standard for Physical Security Risk Management
    b. Appendix A: General Information Flow

**Enquiries**

22) Enquiries are to be forwarded to the Manager, PSS

CBSA-ASFC_DSO_Physical_Security-Securite_Materielle CBSADSOSecurity@cbsa-asfc.gc.ca



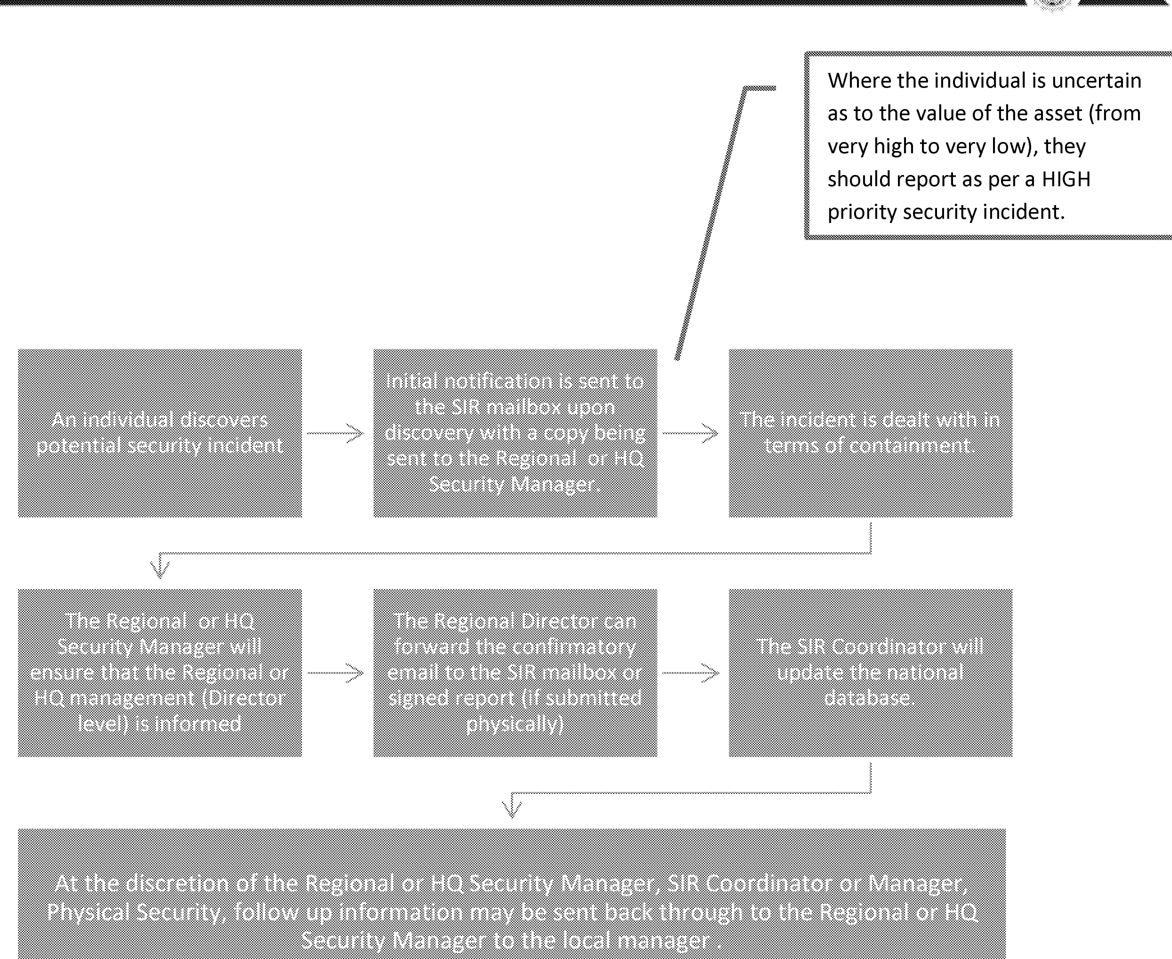
**Appendix A – General Flow of Submission**

This appendix describes the information flow associated with Security Incident Reporting:

- An individual discovers a potential security incident.
- The initial notification is sent to the SIR mailbox upon discovery with a copy being sent to the Regional or HQ Security Manager.
    - Where the individual is uncertain as to the value of the asset (from very high to very low), they should report it as though it were a HIGH priority security incident.
- The incident is dealt with in terms of containment.
- When the incident is contained, then the SIR is submitted as per the instruction above.
    - The Regional or HQ Security Manager will ensure that the Regional or HQ management (director level) is informed.
    - The Corporate Program Service Director can forward the confirmatory email to the SIR mailbox or signed report (if submitted physically) with a copy sent to Regional or HQ Security
    - The SIR Coordinator will update the national database.
- At the discretion of the Regional or HQ Security Manager, SIR Coordinator or Manager, PSS, follow up information may be sent back through the Regional or HQ Security Manager to the local manager.

Note: With respect to file numbers, Regions or HQ may assign file numbers for internal reference. These are to be included on the submission; however, it should be noted that the official number that will be used by the physical security program will be the automatically-generated number in the data management system (IAPRO).






At the discretion of the Regional or HQ Security Manager, SIR Coordinator or Manager, Physical Security, follow up information may be sent back through to the Regional or HQ Security Manager to the local manager .

Agence des services frontaliers du Canada
Canada Border Services Agency



# Norme pour le signalement des incidents de sécurité

PROTECTION • SERVICE • INTÉGRITÉ




Agence des services frontaliers du Canada | Canada Border Services Agency



Cette norme entre en vigueur le 2 février 2015.

**Objet**

1) La présente norme vise à fournir à l'Agence des services frontaliers du Canada (ASFC) une approche structurée pour assurer la mise en œuvre et l'établissement du signalement efficace des incidents de sécurité.

**But**

2) Le présent document a pour but de définir le signalement approprié des incidents de sécurité. Le signalement exhaustif et rapide des incidents de sécurité est essentiel à la capacité de l'Agence de contenir, d'atténuer et de gérer les actes ou les conditions susceptibles de présenter un éventail de risques pour le personnel, les biens, les renseignements et les opérations de l'Agence, et de prendre les mesures qui s'imposent.

**Portée**

3) La présente norme pour le signalement des incidents de sécurité s'applique à toutes les personnes, peu importe leur statut d'emploi, ainsi qu'à toutes les opérations ou à tous les biens sensibles de l'ASFC, y compris ceux qui lui sont confiés par un tiers.
4) C'est à noter que la présente norme ne porte pas sur les exigences en matière de rapports du Centre des opérations frontalières (COF), de Santé et sécurité au travail (SST) ou d'autres programmes. Pour obtenir une orientation propre à ces exigences, prière de communiquer avec les gestionnaires responsables de ces programmes.

**Catégories d'incidents**

5) Les incidents de sécurité englobent ce qui suit :
   a) ***Menaces –*** Tout acte ou toute condition susceptible de présenter un risque de perte (y compris la communication non autorisée, la perturbation et le préjudice) pour le personnel, les biens, les renseignements ou les opérations de l'ASFC. Les menaces diffèrent des incidents de sécurité et des atteintes à la sécurité, étant donné qu'elles n'ont pas encore eu d'incidence sur l'Agence, son personnel ou ses opérations.
   b) ***Violations*** – Tout acte ou toute condition (intentionnel ou non) qui entraîne le contournement d'un contrôle de sécurité ou la réduction de sa capacité de répondre aux attentes de la direction à l'égard de la gestion des risques pour la sécurité matérielle.







c) ***Incidents*** – Tout événement ou toute condition constatée qui comporte l'exploitation d'une vulnérabilité par une menace, mais qui n'a causé aucun préjudice apparent (communication, perturbation, modification, perte).

d) ***Atteintes*** – Tout événement ou toute condition constatée qui comporte l'exploitation apparente d'une vulnérabilité (ou l'équivalent) par une menace, et qui a causé **une perte ou un préjudice défini et mesurable**.

6) Il existe quatre catégories d'incidents :

a) ***Incidents critiques*** – Il s'agit d'incidents ayant causé un préjudice pour le personnel, selon la définition du Groupe de travail sur la gestion des incidents critiques (GTGIC). Il ne faut pas confondre ces incidents avec les questions concernant l'infrastructure critique ou les services essentiels.

b) ***Priorité élevée*** – Il s'agit d'incidents ayant eu une incidence sur des biens de valeur **TRÈS ÉLEVÉE** ou **ÉLEVÉE**, selon la méthode d'évaluation harmonisée des menaces et des risques proposée par la GRC et le CSTC, tableaux B-2 et B-3, pages B-7 et B-8 de la norme publiée à : http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf

c) ***Priorité moyenne*** – Il s'agit d'incidents ayant eu une incidence sur des biens de valeur MOYENNE à FAIBLE, selon la méthode d'évaluation harmonisée des menaces et des risques proposée par la GRC et le CSTC, tableaux B-2 et B-3, pages B-7 et B-8 de la norme publiée à : http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf
Les priorités moyennes comprennent en outre les *menaces* susceptibles de présenter un risque (non immédiat) de préjudice pour le personnel ou de perte de biens de valeur ÉLEVÉE.

d) ***Incidents administratifs*** – Il s'agit d'incidents ayant eu une incidence sur des biens de valeur TRÈS FAIBLE.

Nota : Lorsque des cartes d'identité ou d'autres pièces sont nécessaires pour avoir accès aux biens, le niveau d'accès sert à déterminer si l'incident doit être considéré comme étant à priorité FAIBLE ou MOYENNE. Par exemple, dans le cas d'une carte d'identité donnant accès à un secteur traitant des renseignements « PROTÉGÉ B », une valeur MOYENNE (selon la norme de la GRC) serait accordée, tandis que, dans le cas d'une carte d'identité donnant accès à un secteur verrouillé traitant des renseignements « SECRET », une valeur ÉLEVÉE serait accordée.

**Exigences en matière de rapports**

7) Un rapport d'incident de sécurité (RIS) doit être présenté au moyen du formulaire approuvé de l'ASFC (BSF 152). Dans les circonstances où il n'est pas possible d'utiliser ce formulaire, l'accent est mis sur la fourniture de renseignements exhaustifs.

8) Tous les incidents doivent être signalés de façon exhaustive et rapide afin que l'Agence puisse contenir, atténuer et gérer les actes ou les conditions susceptibles de présenter un éventail de risques pour le personnel, les biens (y compris les renseignements) et les opérations de l'Agence, et prendre les mesures qui s'imposent.



9) Les exigences en matière de rapports sur les **incidents critiques** et les biens de valeur **ÉLEVÉE** sont les suivantes (la définition utilisée est celle proposée par le CTGIC) :
   - L'avis initial de l'incident doit être envoyé par courriel chiffré (ICP) à la boîte aux lettres générale des RIS (Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca) avec copie conforme au gestionnaire de la Sécurité régionale (GSR) ou au gestionnaire de la Sécurité à l'Administration centrale (GSAC) et la mention « Très important ». Si l'incident est signalé au COF, il est possible de répondre à l'exigence en envoyant une copie conforme du courriel à la boîte aux lettres des RIS;
   - Le RIS rempli doit être reçu dans la boîte aux lettres générale des RIS dans les 24 heures suivant la reprise des opérations normales avec une copie envoyé au gestionnaires régionaux de la sécurité (GSR) ou le gestionnaire de la sécurité à l'Administration centrale (GSAC) Lorsque le COF est tenu au courant des événements au fur et à mesure qu'ils se produisent, il est possible de répondre à l'exigence en envoyant une copie conforme du courriel à la boîte aux lettres des RIS. Le RIS rempli doit contenir un résumé exhaustif de l'événement, de ses conséquences, de ses causes profondes ainsi que des mesures de suivi ( y compris les mesures correctives).

     Nota : Des questions complémentaires pourraient être reçues par l'intermédiaire du GSR ou du GSAC ou de l'agent de sécurité du ministère (ASM).

     Nota : Le GASC a le même rôle que le GSR, cependant dans l'AC, le GASC ne doit pas confondre avec les rapports d'incidents de sécurité de l'AC : Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca

10) Les incidents à **priorité élevée** (dans les cas où le COF n'est pas avisé) doivent être signalés comme suit :
   - L'avis initial de l'incident doit être envoyé par courriel chiffré (ICP) à la boîte aux lettres générale des RIS (Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca) avec copie conforme au GSR ou au GSAC.
   - Le RIS rempli doit être envoyé à la boîte aux lettres générale des RIS dans les 24 heures suivant la reprise des opérations normales.
   - Le RIS rempli doit contenir un résumé exhaustif de l'événement, de ses conséquences, de ses causes profondes ainsi que des mesures de suivi (y compris les mesures correctives).

   Nota : Des questions complémentaires pourraient être reçues par l'intermédiaire du GSR ou du GSAC ou de l'ASM.

11) Les incidents à **priorité moyenne** sont signalés comme suit :
   - L'avis initial de l'incident doit être envoyé par courriel chiffré (ICP) à la boîte aux lettres générale des RIS (Security_Incident_Reports-rapports_incidents_de_securite@cbsa-asfc.gc.ca) avec copie conforme au GSR ou au GSAC dans les 24 heures suivant l'incident.







- Le RIS rempli doit être reçu dans les 96 heures suivant la reprise des opérations normales ou, s'il n'y a peu eu perturbation des opérations, dans les 96 heures suivant l'avis initial.
- Le RIS rempli doit contenir un résumé exhaustif de l'événement, de ses conséquences, de ses causes profondes ainsi que des mesures de suivi ( y compris les mesures correctives).

Nota : Des questions complémentaires pourraient être reçues par l'intermédiaire du GSR ou du GSAC.

12) Les incidents **administratifs** doivent être signalés comme suit :
   - Le RIS doit être envoyé au GSR ou au GSAC avec copie conforme à la boîte aux lettres des RIS dans la semaine suivant l'incident initial.
   - Le RIS rempli doit contenir un résumé exhaustif de l'événement, de ses conséquences, de ses causes profondes ainsi que des mesures de suivi ( y compris les mesures correctives).

Nota : Des questions complémentaires pourraient être reçues par l'intermédiaire du GSR ou du GSAC.

13) Voici les renseignements généraux à inclure :
   - Réponses aux questions « qui », « quoi », « quand », « où » et « comment » pertinentes pour l'incident,
   - Identification du bien (numéro de série, numéro d'identification unique),
   - Tout coût connexe (remplacement, solution provisoire), le cas échéant,
   - Nature et durée de toute perturbation, le cas échéant,
   - Toute mesure corrective ou d'atténuation prise, et
   - Numéros de dossier pour les rapports de police (le cas échéant), du CIPC, etc., qui pourraient être pertinents dans le cadre d'une enquête.

**Duplication de rapports**

14) Lorsqu'un rapport officiel traitant des renseignements ci-dessus est présenté à un autre secteur de l'Agence, une copie conforme de ce rapport peut être envoyée, et l'exigence relative aux RIS peut être considérée comme ayant été respectée. Il pourrait y avoir un suivi de la sécurité de l'AC ou des régions, qui doivent s'assurer qu'il ne manque aucun renseignement.

**Rôles et responsabilités**

15) Agent de sécurité ministériel (ASM)

   L'ASM est responsable du programme de sécurité global à l'ASFC.

16) Directeur, Division de l'infrastructure et de la sécurité de l'information (DISI)



Le directeur, DISI, est responsable de la mise en œuvre, de la gestion stratégique et de la surveillance du programme de sécurité matérielle pour l'Agence. De plus, il s'assure que les priorités du programme demeurent conformes à celles de l'Agence.

17) Gestionnaire, Section de la sécurité matérielle (SSM)

Le gestionnaire, SSM, est responsable de la gestion opérationnelle du programme de sécurité matérielle. Il incombe au gestionnaire :

- D'élaborer les processus et les stratégies pour la gestion effective des incidents de sécurité;
- D'élaborer, mettre en œuvre et communiquer la norme à appliquer pour le signalement des incidents de sécurité, notamment la capacité de demander des renseignements de façon officielle au nom de l'ASM afin de déterminer la portée et les répercussions de l'incident;
- D'agir à titre d'autorité fonctionnelle pour l'analyse de l'incidence sur la sécurité matérielle à l'Agence;
- D'assurer la continuité et l'application uniforme à l'échelle de l'ASFC;
- D'assurer l'uniformité à l'échelle nationale.

18) Coordonnateur des incidents de sécurité (CIS), SSM

Il incombe au CIS :

- D'effectuer l'évaluation préliminaire, l'analyse et la validation de tous les incidents de sécurité entrants ;
- De contrôler et d'assurer la qualité et l'intégrité des renseignements ;
- De prendre des mesures de suivi pour les incidents de sécurité en lançant un système de suivi, en consultant les clients à l'AC et dans la région, en vérifiant toutes les nouvelles données, en mettant à jour la base de données sur la sécurité et en établissant des rapports supplémentaires, au besoin ;
- D'analyser l'incidence et de déterminer les tendances; de formuler des conclusions préliminaires et de les présenter au gestionnaire de la SSM à des fins d'enquête et d'évaluation futures ; et
- D'offrir une orientation et de l'aide à la haute direction, aux clients et aux bureaux régionaux en ce qui concerne les méthodes de collecte de données, la validation de données, la détection d'incohérences et l'obtention d'éclaircissements, ainsi que le regroupement de données en vue de l'établissement de divers rapports.

Gestionnaire de la Sécurité régionale (GSR) et gestionnaire de la Sécurité à l'AC (GSAC)

19) Le GSR et le GSAC possèdent les pouvoirs délégués par l'ASM pour la prestation du programme de sécurité matérielle, et agissent au nom du gestionnaire de la SSM dans la région et à l'AC. Le GSR ou le GSAC :

- S'assure que tous les RIS sont exhaustifs ;







- Analyse, évalue et valide les renseignements entrants, tout en assurant le suivi approprié pour tout renseignement manquant au CIS ;
- Recommande des mesures correctives, au besoin ;
- S'assure que toutes les directives, les politiques, les normes, les lignes directrices et les procédures liées à la sécurité matérielle sont respectées dans la région ou au CIS ;
- Aide à mener des vérifications, à faire des rapprochements et à répondre à des demandes de la SSM ;
- Veille à ce que la région soit sensibilisée aux incidents de sécurité et reçoive la formation connexe.

**Conséquences**

20) Assurer le signalement rapide des incidents de sécurité permet de veiller à ce que le programme de sécurité matérielle soit au courant des questions pertinentes pour l'Agence, et puisse se concentrer sur ces questions. Le défaut de prendre des mesures raisonnables pour signaler un incident de sécurité peut entraîner une poursuite administrative, civile ou criminelle selon la nature de l'incident et les conclusions de toute enquête menée par la suite.

**Documents connexes**

21) La présente norme découle de la Directive sur la sécurité matérielle et doit être appliquée de concert avec ce qui suit :
    a. Norme sur la gestion du risque en matière de la sécurité matérielle
    b. Annexe A : Flux d'information général

**Demandes de renseignements**

22) Les demandes de renseignements doivent être adressées au gestionnaire de la SSM à :

CBSA-ASFC_DSO_Physical_Security-Securite_Materielle CBSADSOSecurity@cbsa-asfc.gc.ca



**Annexe A – Flux d'information général**

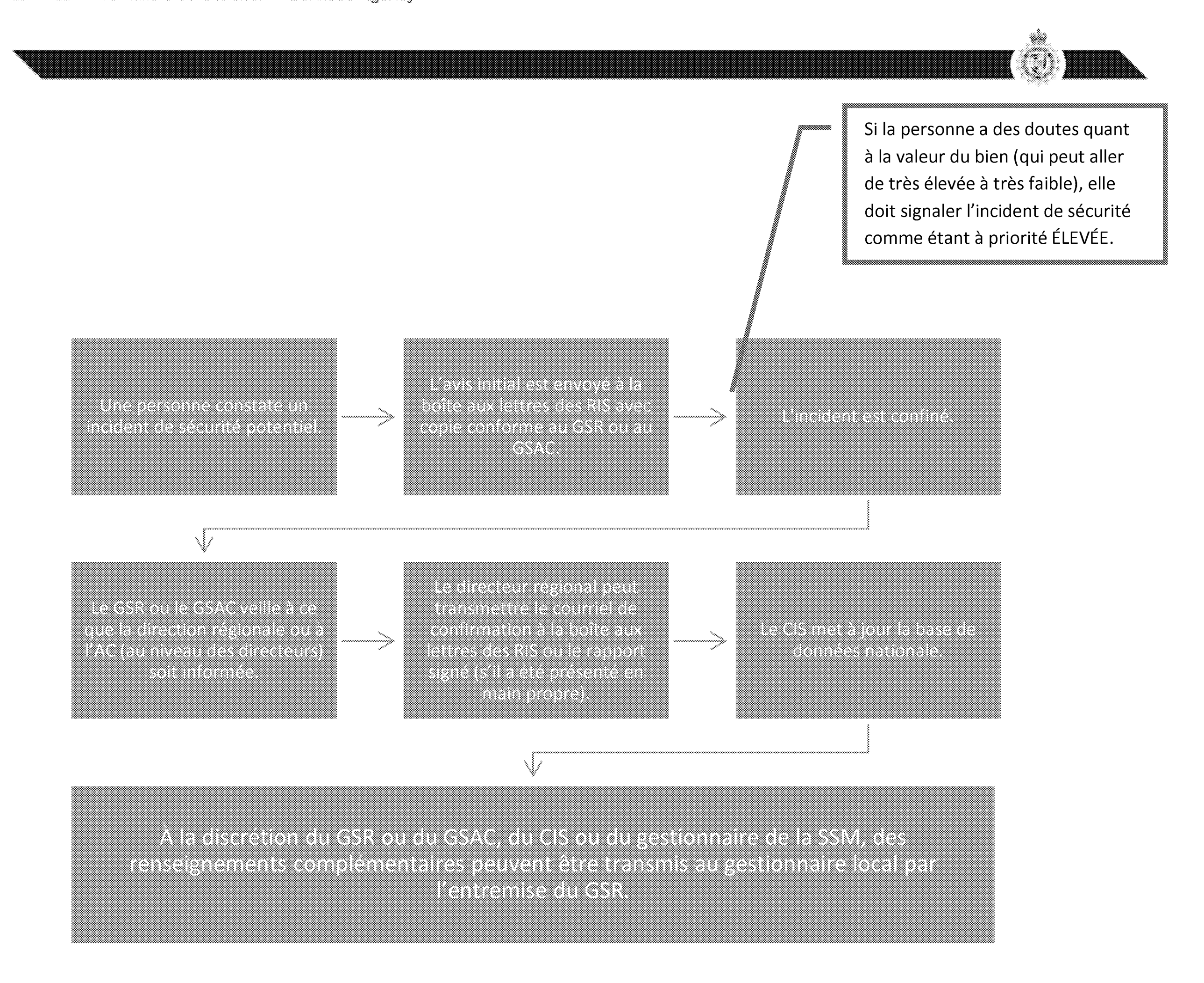
Dans la présente annexe, est décrit le flux d'information associé au signalement des incidents de sécurité :

- Une personne constate un incident de sécurité potentiel.
- L'avis initial est envoyé à la boîte aux lettres des rapports sur les incidents de sécurité (RIS) avec copie conforme au gestionnaire de la Sécurité régionale (GSR) ou au gestionnaire de la Sécurité à l'AC (GSAC).
    - Si la personne a des doutes quant à la valeur du bien (qui peut aller de très élevée à très faible), elle doit signaler l'incident de sécurité comme étant à priorité ÉLEVÉE.
- L'incident est contenu.
- Une fois l'incident contenu, le RIS est envoyé selon les directives ci-dessus.
    - Le GSR ou le GSAC veille à ce que la direction régionale ou à l'AC (au niveau des directeurs) soit informée.
    - Le directeur des Services organisationnels et des programmes peut transmettre le courriel de confirmation à la boîte aux lettres des RIS ou le rapport signé (s'il a été présenté en main propre) avec une copie envoyé à la sécurité de l'AC ou des régions.
    - Le CIS met à jour la base de données nationale.
- À la discrétion du GSR ou du GSAC, du CIS ou du gestionnaire de la SSM, des renseignements complémentaires peuvent être transmis au gestionnaire local par l'entremise du GSR ou du GSAC.

Nota : En ce qui concerne les numéros de dossier, la région ou l'AC peut attribuer des numéros de dossier pour usage interne. Ces numéros doivent être inclus dans l'information présentée; cependant, le numéro officiel qui est utilisé par le programme de sécurité matérielle est celui produit automatiquement par le système de gestion des données (IAPro).






Si la personne a des doutes quant à la valeur du bien (qui peut aller de très élevée à très faible), elle doit signaler l'incident de sécurité comme étant à priorité ÉLEVÉE.
Une personne constate un incident de sécurité potentiel.
L'avis initial est envoyé à la boîte aux lettres des RIS avec copie conforme au GSR ou au GSAC.
L'incident est confiné.
Le GSR ou le GSAC veille à ce que la direction régionale ou à l'AC (au niveau des directeurs) soit informée.
Le directeur régional peut transmettre le courriel de confirmation à la boîte aux lettres des RIS ou le rapport signé (s'il a été présenté en main propre).
Le CIS met à jour la base de données nationale.
À la discrétion du GSR ou du GSAC, du CIS ou du gestionnaire de la SSM, des renseignements complémentaires peuvent être transmis au gestionnaire local par l'entremise du GSR.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for Controlled Assets

PROTECTION • SERVICE • INTEGRITY

Canadä



This Standard takes effect on February 2, 2015.

**Purpose**

1) The purpose of this standard is to provide the Canada Border Services Agency (CBSA) with a structured approach to ensure the implementation and establishment of effective internal controls for controlled assets.

**Intent**

2) The intent of this document is to define the proper administration of policy, issuance, control storage and management of CBSA controlled assets throughout their lifecycle. An effective system of security controls must remain consistently in force so as to ensure that the level of trust (internal and public) does not fall below the minimum levels of trust or confidence associated with the asset.

**Application**

3) The *Standard for Controlled Assets* is applicable to all persons, regardless of their employment status, that seek or may be given access to Controlled Assets.

**Requirements**

4) Design - The design of any controlled asset must take into account the following:

- The ability to uniquely identify the asset;
- The ability to protect the asset itself against unauthorized access, modification or damage as appropriate; and,
- The ability to protect the message, mark or other impression conveyed through the appropriate use of the asset against unauthorized duplication, modification, or removal.

5) The design phase of any Controlled Asset must also take into account the following scenarios:

- Removal of the asset from service and modification of any sensitive parts or elements so as to protect the asset from being returned into service surreptitiously;
- Emergency destruction or modification of the asset to keep the asset (and its capabilities) from falling into hostile or competitive hands; and,
- The ability to detect attempts to gain access to sensitive elements of the asset.







6) The Physical Security Section (PSS) may integrate certain security features into the controlled asset as a means of assisting in the determination of its authenticity. Where such controls are put in place, any documentation or means of replicating the controls (such as dies, etc.) are to be protected against unauthorized disclosure, unauthorized modification or loss of availability. These themselves become controlled assets and are assigned an asset value (in the physical security context) of HIGH INTEGRITY and, depending on the nature of the asset, may also be assigned a value in the national interest.

***Issuance***

7) To be issued a controlled asset, the individual seeking issuance must be able to clearly demonstrate the following:

- The individual has either a need to have possession of the controlled asset in order to perform an Agency authorized function;
- The individual must possess the requisite level of security screening granted at a level commensurate to the sensitivity of the asset; and,
- The individual must have acknowledged an understanding and commitment to comply with the various controls placed on the controlled asset.

8) The issuance process for all controlled assets must maintain records demonstrating consistent control over the controlled asset. This includes, but may not necessarily be limited to, the following:

- The date and time on which the controlled asset was issued;
- The unique identifier and type of controlled asset;
- The location at which the controlled asset was issued;
- The identity of the individual issuing the controlled asset; and,
- The identity of the individual being issued the controlled asset.

9) Each individual being issued a controlled asset must complete appropriate forms as understanding and accepting the following:

- That the controlled asset remains the property of the Agency;
- That the controlled asset must be returned upon demand; and,
- That the controlled asset may only be used for the purpose which it is being issued.



10) All issuances and returns of controlled asset must be documented. Such documents are to be retained so as to be able to demonstrate the continuous custody of the controlled asset and up to two years past its last administrative use.

11) Where controlled assets are being issued in accordance with Agency policies, the onus is on the requesting Custodian or Manager to demonstrate that all the conditions of issuance have been met before a Security Officer/Specialist can issue.

***Storage***

12) Controlled assets must be stored in such a way that the trust in their integrity has not been compromised through unauthorized access, modification, or use.

13) The following must be maintained at all times:
    - An individual must be clearly identified who is responsible for monitoring the storage requirements;
    - An inventory that clearly lists all controlled asset shall be maintained. While not in immediate service (i.e. when in storage), the individual identified above becomes the *de facto* custodian of the controlled asset;
    - The approved secure container in which the controlled asset are stored must be approved by the Physical Security Section (PSS); and,
    - The storage container should be subject to two-person integrity controls and approved by PSS.

***Supply Chain***

14) Controlled assets shall only be procured through the PSS. The PSS will enter the asset into the main inventory.

15) Controlled assets, in all phases of its development and lifecycle, are to ensure that all components included in the controlled assets are sourced from trustworthy suppliers with the proper level of clearance as approved by PSS.

16) Where an approved supplier is used to maintain the controlled asset, there must be a control process to ensure that all sensitive materials are either packaged or returned; and,

17) Controlled assets shall only be repaired or maintained through suppliers approved by PSS.

***Shipping***

18) Custodians (the sender) shipping controlled assets are required to adhere to the following:



- Ship the controlled asset to the expected recipient by a bonded courier approved by the PSS and the shipment must be traceable with tracking number and chain of signature at all times;
- Ensure that all appropriate documentation to be included with the shipment and to acknowledge the shipment (by way of return receipt) is included
- Package controlled assets in a sealed box or container and clearly marked "PROTECTED";
- Ensure the sealed box or container is wrapped a second time in heavy wrapping paper and taped securely to prevent easy access;
- Ensure there are no security markings on the outer package;
- Ensure the name and address of the recipient are clearly marked on the front of the package;
- Ensure a return address is inscribed on the front of the package in the upper left hand corner; and,
- Ensure no other information has been inscribed on the exterior of the package.
- For transport regarding information assets please refer to the *Standard for Storage and Transport of Information Assets* or for the transport of sensitive information please refer to *Standard for the Transmittal of Sensitive Information/Assets*.

**Roles and Responsibilities**

*Department Security Officer (DSO)*

19) The Department Security Officer is responsible for the overall Security program within CBSA. The DSO delegates the Manager of Physical Security Section (PSS) the responsibility of managing the national Controlled Asset program. The DSO also delegates the task of managing the Regional Controlled Asset Program to the Regional Security Manager (RSM).

*Director, Infrastructure and Information Security*

20) The Director provides strategic direction over the Controlled Asset program, ensuring that the program remains aware and aligned with the overall strategic direction of the Agency.

*Manager, Physical Security Section (PSS)*

21) The Manager of PSS is responsible for all controlled assets across CBSA. All decisions pertaining to the lifecycle management of the controlled asset portfolio remain the manager's responsibility in conjunction with the DSO.

*National Controlled Asset Coordinator*

22) The National Controlled Asset Coordinator is the national functional expert and the delegated authority under the manager of PSS. The National Controlled Asset Coordinator:



- Provides all guidance and direction on controlled assets and associated systems;
- Supplies all regions with supplies for controlled assets;
- Supplies all regions with controlled assets;
- Manages and writes the contracts for controlled assets;
- Ensures national compliance with all associated policies, standards and guidelines for controlled assets as well as associated legislation;
- Provides guidance and advice to many levels of management in regard to controlled asset policies, standards and guidelines;
- Provides guidance and advice to many levels of management in regards to controlled asset reports;
- Conducts Audits and reconciliations of the controlled asset inventories across CBSA;
- Troubleshoots and manages controlled asset systems and software as well as all associated hardware;
- Manages the National Controlled Asset database (CAS) and ensures accuracy;
- Writes the standards, guidelines and operating procedures for controlled assets;
- Investigates all cases of security incidents involving controlled assets;
- Collects and provides all statistics requested by Management;
- Ensures quality control of controlled assets;
- Liaises with all internal and external clients in relation to controlled assets;
- Assesses the program on a regular basis to recommend improvements;
- Develops processes and strategies for controlled assets;
- Ensures continuity and consistent application across CBSA; and,
- Manages inventory of controlled assets nationally.

*Regional Security Manager (RSM) and Regional Security Manager in HQ*

23) The Regional Security Manager (RSM) is the delegated Regional authority by the DSO for controlled assets who acts on behalf of the Manager of PSS within the Region. All controlled assets in the Regions are the responsibility of the RSM as well as the maintenance and updating of all systems and reports. The RSM:
    - Ensures that the National Controlled Asset coordinator and the Manager of PSS are aware of any and all concerns or issues associated with controlled assets;
    - Ensures that Custodians have the necessary knowledge and skills required to administer the controlled asset program;
    - Ensures that all assets are stored and handled as outlined in the appropriate policies and standards;
    - Ensures Regional compliance with all related directives, policies, standards, guidelines and procedures concerning controlled assets;
    - Provides assistance in the completion of audits, reconciliations and requests initiated by the PSS;



- Ensures that all security incidents related to controlled assets are reported as defined in the CBSA policy requirements; and,
- Ensures regional awareness and training related to controlled assets.

*Regional Security Officer/Specialist*

24) The Regional Security Officer/Specialist is the Regional Functional expert delegated by the Regional Security Manager to carry out the National Controlled Asset program. The Regional Security Officer:
    - Ensures that CAS is up to date, accurate, and all information is keyed in CAS;
    - Ensures all controlled assets are stored as per storage requirements;
    - Manages Regional controlled asset inventories;
    - Trains site coordinators on the use of controlled formss and controlled asset procedures;
    - Analyzes, assesses and validates incoming information on controlled assets, and forms, reconcile discrepancies and follows-up on reported information;
    - Follows up on missing information on controlled forms before submittal to HQ;
    - Ensures that all BSF208 and BSF203 are completed and vetted for accuracy before submittal to HQ;
    - Ensures that all BSF208 and BSF203 are sent to the PSS National Controlled Asset Coordinator within the 30 calendar day timeframe;
    - Ensures compliance with all associated policies for the controlled assets within their Region;
    - Ensures that all requests by other Regional Security Offices are dealt with in a timely fashion;
    - Communicates all transfers of controlled assets to the appropriate regional security office and ensuring the safe arrival in conjunction with the shipping requirements;
    - Ensures that all controlled assets are shipped in accordance to the Standard and policy;
    - Conducts maintenance on the ID card computer and associated software fixes;
    - Has knowledge of controlled asset systems;
    - Initiates or conduct all Regional investigations on controlled assets;
    - Conducts regular audits and reconciliations;
    - Complies with all audits, reconciliations, and requests initiated by the PSS; and,
    - Notifies the RSM and National Controlled Assets Coordinator of any compromise of assets.

*Chief/Superintendent*

25) The Chief/Superintendent is the delegated Port authority for controlled assets who acts on behalf of the Regional Security Manager in the Region. All controlled assets at the port are the responsibility of the Chief/Superintendent, who:



- Ensures all Custodians are compliant with the associated policies and standards on controlled assets;
- Ensures all controlled assets are stored as per storage requirements;
- Ensures all Custodians fill out the BSF152, BSF208, BSF203 in their entirety with full details;
- Ensures all transfer of assets are documented accordingly and are reported to the respective Regional Security Office;
- Ensures all new personnel transferring into the port have reported all incoming controlled assets to the respective Regional Security Office;
- Complies with all audits and reconciliations initiated by Regional Security or the PSS; and,
- Notifies Regional Security of any compromise of controlled assets.

*Site Coordinator*

26) The Site Coordinator is the delegated individual by the Chief or Superintendent to control the inventory of controlled assets at the port. Should a Site Coordinator not be identified to PSS then the Chief/Superintend must assume these duties. The Site Coordinator:

- Ensures all logs are keep up to date and accurate;
- Ensures all inventories of controlled assets are stored in accordance with storage requirements;
- Complies with all audits and reconciliations initiated by Regional Security or the PSS; and,
- Ensures all controlled forms are completed, accurate and not missing any information.

*Custodian*

27) The Custodian is bound by the code of conduct and all associated controlled asset policies, operational policies, program policies and Uniform policies and standards as well as the Policy on security incident reporting. The Custodian:
- Ensures the completion of the controlled forms (BSF208, BSF203, BSF270 and the BSF152);
- Ensures the completion of all controlled forms are done in a timely manner and submitted to Regional Security once a change to the status of the controlled asset has changed;
- Ensures all controlled forms are accurate and fully completed before submittal;
- Ensures the storage of controlled asset in conjunction with all policies and standards when the asset is with individual and when locking up;



- Safeguards information and assets under their control whether working on- or off-site in conjunction with regulations;[1]
- Notifies respective Regional Security Office of any transfer and follows direction provided by the Regional Security Officer or Specialist before transferring; and,
- Maintains awareness of controlled asset concerns and issues to ensure their actions do not compromise departmental security.[2]

**Enquiries**

28) Enquiries are to be forwarded to the Manager, Physical Security
CBSADSOSecurity@cbsa-asfc.gc.ca

**Appendix A – Definitions**

**Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.**

**Controlled Forms**

The Controlled Forms are the forms used to track all movements of the Controlled Asset as well as all incidents pertaining to the Controlled Asset.

BSF208: Controlled Asset Form

BSF203: Status Designation CBSA Port Stamp – Sample Impressions

BSF152: Security Incident Report

BSF270: Custodian Departure/Transfer Notification

BSF672: Daily Port Stamp Allocation

[1] 6.1.27 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579&section=text
[2] 6.1.30 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579&section=text

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme visant les biens contrôlés



Cette norme entre en vigueur le 2 février 2015.

**Objectif**

1) La présente norme vise à fournir à l'Agence des services frontaliers du Canada (ASFC) une approche structurée afin d'assurer l'établissement et la mise en place de contrôles internes efficaces à l'égard des biens contrôlés.

**Objet**

2) Le présent document vise à définir des concepts liés aux biens contrôlés de l'ASFC qui entrent en compte tout au long du cycle de vie, soit l'administration des politiques, la délivrance, l'entreposage et la gestion. Il doit y avoir un système efficace de contrôles de sécurité en place en tout temps pour veiller à ce que le niveau de confiance (à l'interne et au sein du public) soit égal ou supérieur au niveau de confiance associé au bien.

**Mise en application**

3) La Norme visant les biens contrôlés s'applique à toute personne, peu importe son emploi, qui veut ou peut obtenir accès à des biens contrôlés.

**Exigences**

4) Conception – il faut tenir compte des éléments suivants pour tous les biens contrôlés :

- Capacité de désigner le bien de façon exclusive;
- Capacité de protéger convenablement le bien contre une modification ou un accès non autorisé ou des dommages;
- Capacité de protéger le message, la marque ou l'impression créée par l'utilisation adéquate du bien contre une reproduction, une modification ou un enlèvement non autorisé.

5) L'étape de conception de tous biens contrôlés doit également tenir compte des situations suivantes :

- Mise hors service du bien et modification de tout élément ou composante de nature délicate en vue de protéger le bien contre la remise en service clandestine;
- Destruction ou modification d'urgence du bien pour prévenir que le bien (et ses fonctions) ne tombe sous la main de personnes aux intentions hostiles ou compétitives;
- Capacité de déceler les personnes qui tentent d'avoir accès à des composantes délicates du bien.







6) La Section de la sécurité matérielle (SSM) peut intégrer certaines fonctions de bien de sécurité contrôlé qui serviront à en déterminer l'authenticité. Lorsque de telles fonctions sont mises en place, tout document ou moyen servant à reproduire le contrôle (p. ex. filières) doit être protégé contre la divulgation ou la modification non autorisée ou la perte de disponibilité. Ces fonctions deviennent des biens contrôlés et sont considérées comme un bien (dans le contexte de la sécurité matérielle) d'INTÉGRITÉ ÉLEVÉE et selon la nature du bien, possiblement d'intérêt national.

***Délivrance***

7) Une personne cherchant à obtenir un bien de sécurité contrôlé doit être en mesure de démontrer les éléments suivants :

- La personne doit avoir besoin du bien contrôlé pour réaliser des fonctions autorisées par l'ASFC;
- La personne doit avoir la cote de sécurité requise relativement à la nature délicate du bien;
- La personne doit affirmer comprendre les mesures de contrôles visant le bien de sécurité contrôlé, et elle doit s'engager à les respecter.

8) Le processus de délivrance pour tous les biens contrôlés doit prévoir une tenue de dossier pour montrer le contrôle continu du bien contrôlé. Les renseignements suivants doivent être consignés :

- La date et l'heure à laquelle le bien contrôlé a été délivré;
- L'identificateur unique du bien et le type de bien contrôlé;
- L'endroit où le bien contrôlé a été délivré;
- Le nom de la personne qui a délivré le bien contrôlé;
- Le nom de la personne qui a obtenu le bien contrôlé.

9) Chaque personne qui obtient un bien de sécurité contrôlé doit remplir les formulaires requis pour confirmer qu'elle comprend et qu'elle accepte ce qui suit :

- Le bien contrôlé demeure la propriété de l'ASFC;
- Le bien contrôlé doit être retourné dès que l'ASFC en fait la demande;
- Le bien contrôlé doit être utilisé uniquement aux fins auxquelles il a été délivré.

10) Toute délivrance et tout retour d'un bien contrôlé doivent être consignés. Les documents doivent être conservés de façon à ce qu'il soit possible de consulter l'historique complet du bien contrôlé, jusqu'à deux ans après la dernière utilisation à des fins administratives.

11) En ce qui concerne la délivrance de biens contrôlés conformément aux politiques de l'ASFC, il incombe au responsable des biens contrôlés (responsable des biens) ou au gestionnaire qui en a fait







la demande de démontrer que toutes les conditions de délivrance ont été respectées avant qu'un agent de sécurité/spécialiste puisse délivrer des biens.

*Entreposage*

12) Les biens contrôlés doivent être entreposés de façon à préserver la confiance à l'égard de l'intégrité du bien, c'est-à-dire de façon à éviter qu'il ne soit compromis par une modification, une utilisation ou un accès non autorisé.

13) Les éléments suivants doivent être respectés en tout temps :
- Une personne doit être désignée comme responsable de la surveillance des exigences relatives à l'entreposage;
- Il est nécessaire de tenir un inventaire qui énumère clairement tous les biens contrôlés. La personne susmentionnée devient le responsable *de facto* des biens contrôlés qui ne sont pas en service immédiat (p. ex. biens entreposés);
- Le conteneur sûr approuvé dans lequel sont entreposés les biens contrôlés doit être approuvé par la Section de la sécurité matérielle (SSM);
- Le conteneur doit faire l'objet d'un contrôle d'intégrité assurée par deux personnes et doit être approuvé par la SSM.

*Chaîne d'approvisionnement*

14) Les biens contrôlés peuvent seulement être acquis par l'entremise de la SSM. La SSM inscrira le bien dans l'inventaire principal.

15) À toutes les étapes de développement et de cycle de vie des biens contrôlés, il est nécessaire de veiller à ce que toutes les composantes proviennent de fournisseurs fiables munis de la cote de sécurité requise approuvée par la SSM.

16) En ce qui concerne le recours à un fournisseur pour l'entretien d'un bien contrôlé, il doit y avoir une vérification pour s'assurer que tout le matériel de nature délicate soit emballé ou retourné.

17) Les biens contrôlés doivent seulement être réparés ou entretenus par des fournisseurs approuvés par la SSM.

*Expédition*

18) Le responsable des biens (expéditeur) qui expédie les biens contrôlés doit respecter les consignes suivantes :







- Expédier les biens contrôlés au destinataire prévu au moyen d'un service de messagerie assurée qui a été approuvé par la SSM et veiller à ce que l'envoi soit repérable à l'aide d'un numéro de repérage et une chaîne de signature en tout temps;
- Veiller à ce que tous les documents pertinents requis et les documents servant à accuser réception de l'envoi (accusé de réception) soient compris dans l'envoi;
- Emballer les biens contrôlés dans une boîte ou un contenant scellé portant clairement la marque « PROTÉGÉ »;
- Veiller à ce que la boîte ou le contenant scellé soit ensuite recouvert d'un papier d'emballage robuste solidement retenu par du ruban adhésif afin d'empêcher tout accès facile;
- S'assurer qu'il n'y a aucune marque de sécurité sur l'extérieur du colis;
- Veiller à ce que le nom et l'adresse du destinataire soient clairement indiqués sur le colis;
- Veiller à ce que l'adresse de l'expéditeur figure sur le coin supérieur gauche du colis;
- Veiller à ce qu'aucun autre renseignement ne figure sur l'extérieur du colis.
- Pour le transport de ressources d'information, veuillez-vous reporter à la *Norme sur le stockage et le transport de ressources d'information* ou pour le transport d'informations sensibles, veuillez-vous référer à la *Normes sur la transmission de renseignements et de ressources de nature délicate.*

**Rôles et responsabilités**

*Agent de sécurité du ministère (ASM)*

19) L'agent de sécurité du ministère est responsable de l'ensemble du programme de sécurité de l'ASFC. L'ASM délègue au gestionnaire de la Section de la sécurité matérielle (SSM) la responsabilité de gérer le programme national des biens contrôlés. Il délègue également au gestionnaire régional de la sécurité (GRS) ou le gestionnaire de la Sécurité à l'AC (GSAC) la responsabilité de gérer le programme régional des biens contrôlés.

*Directeur, Division de l'infrastructure et de la sécurité de l'information*

20) Le directeur fournit une orientation stratégique du programme de biens contrôlés, et veille à ce que le programme tienne compte de l'orientation stratégique globale de l'ASFC et à ce qu'il cadre avec celle-ci.

*Gestionnaire, Section de sécurité matérielle (SSM)*

21) Le gestionnaire de la SSM est responsable de tous les biens contrôlés à l'échelle de l'ASFC. Toute décision portant sur la gestion du cycle de vie du portefeuille d'un bien de sécurité contrôlé relève du gestionnaire, et est prise conjointement avec l'ASM.

*Coordonnateur national des biens contrôlés*



22) Le coordonnateur national des biens contrôlés est l'expert fonctionnel national et le pouvoir délégué qui relève du gestionnaire de la SSM. Le coordonnateur national des biens contrôlés:

- fournit conseils et orientation à l'égard des biens contrôlés et des systèmes connexes;
- fournit aux régions les fournitures nécessaires à l'égard des biens contrôlés;
- fournit aux régions les biens contrôlés;
- gère et rédige les marchés visant les biens contrôlés;
- veille au respect de toutes les politiques, les normes et les lignes directrices nationales portant sur les biens contrôlés, ainsi qu'au respect des lois connexes;
- fournit des conseils et une orientation à des gestionnaires de divers niveaux à l'égard des politiques, des normes et des lignes directrices visant les biens contrôlés;
- fournit des conseils et une orientation à des gestionnaires de divers niveaux à l'égard des rapports sur les biens contrôlés;
- réalise des vérifications et des rapprochements de l'inventaire des biens contrôlés à l'échelle de l'ASFC;
- gère les systèmes et les logiciels, ainsi que le matériel connexe, liés aux biens contrôlés et en assure le dépannage;
- gère la base de données nationale des biens contrôlés et veille à l'exactitude des données;
- rédige les normes, les lignes directrices et les procédures opérationnelles visant les biens contrôlés;
- mène une enquête de tous les incidents en matière de sécurité mettant en cause les biens contrôlés;
- recueille et fournit toutes les statistiques demandées par la direction;
- veille au contrôle de la qualité des biens contrôlés;
- assure la liaison avec les clients internes et externes relativement aux biens contrôlés;
- évalue le programme régulièrement en vue de recommander des améliorations;
- élabore des processus et des stratégies à l'égard des biens contrôlés;
- assure la continuité et l'application uniforme à l'échelle de l'ASFC; et,
- gère l'inventaire des biens contrôlés à l'échelle nationale.

*Gestionnaire de la Sécurité régionale (GSR) et gestionnaire de la Sécurité à l'AC (GSAC)*

23) Le Gestionnaire de la Sécurité régionale (GSR) ou le gestionnaire de la Sécurité à l'AC (GSAC) est l'autorité régionale déléguée par l'agent de sécurité du ministère (ASM) pour les biens contrôlés, qui agit au nom du gestionnaire de la Section de la sécurité matérielle (SSM) dans la région. Tous les biens contrôlés à l'échelle régionale, ainsi que l'entretien et l'actualisation des systèmes et des rapports, sont la responsabilité du GRS. Le GRS/GSAC:

- veille à ce que le coordonnateur national des biens contrôlés et le gestionnaire de la SSM soient au fait des préoccupations et des questions liées aux biens contrôlés;
- veille à ce que les responsables des biens possèdent les connaissances et les compétences requises pour exécuter le programme des biens contrôlés;







- s'assure que tous les biens sont entreposés et manipulés tel qu'il est précisé dans les politiques et les normes connexes;
- assure la conformité, à l'échelle régionale, avec les directives, les politiques, les normes, les lignes directrices et les procédures sur les biens contrôlés connexes;
- participe à la réalisation des vérifications, des demandes et des rapprochements lancés par la SSM;
- veille à ce que tous les incidents de sécurité liés aux biens contrôlés soient signalés tel qu'il est décrit clairement dans les exigences de la politique de l'ASFC;
- assure une sensibilisation et une formation à l'échelle régionale relativement aux biens contrôlés.

*Agent régional de sécurité/spécialiste*

24) L'agent régional de sécurité/ spécialiste est l'expert fonctionnel régional délégué par le GRS et chargé d'exécuter le programme national des biens contrôlés. L'agent régional de sécurité :

- veille à ce que les renseignements figurant dans la base de données nationale des biens contrôlés soient exacts et à jour et veille à ce que tous les renseignements soient entrés dans la base de données;
- s'assure que tous les biens contrôlés sont entreposés en fonction des exigences en matière d'entreposage;
- gère les inventaires régionaux des biens contrôlés;
- offre une formation aux coordonnateurs locaux sur l'utilisation des formulaires de contrôle et l'application des procédures liées aux biens contrôlés;
- analyse, évalue et valide les renseignements reçus sur les biens contrôlés et les formulaires, corrige les écarts et assure le suivi des renseignements fournis;
- fait un suivi relativement aux renseignements manquants sur les formulaires de contrôle avant de présenter les formulaires à DSNP;
- veille à ce que tous les formulaires BSF208 et BSF203 soient remplis et à ce que leur exactitude soit vérifiée avant de les présenter à DSNP;
- s'assure que tous les formulaires BSF208 et BSF203 sont envoyés au coordonnateur national des biens contrôlés de la SSM dans un délai de 30 jours civils;
- assure la conformité avec les politiques connexes sur les biens contrôlés à l'échelle régionale;
- veille à ce que les demandes présentées par d'autres bureaux régionaux de sécurité soient traitées en temps opportun;
- communique tous les transferts de biens contrôlés au bureau régional de sécurité approprié et veille à la bonne arrivée des biens conformément aux exigences en matière d'expédition;
- s'assure que tous les biens contrôlés sont expédiés conformément aux normes et aux politiques;
- met à niveau l'ordinateur utilisé pour les cartes d'identité et installe les correctifs connexes;







- connaît bien les systèmes liés aux biens contrôlés;
- lance ou mène les enquêtes régionales sur les biens contrôlés;
- effectue régulièrement des vérifications et des rapprochements;
- respecte les vérifications, les rapprochements et les demandes lancées par la SSM;
- avise le GRS et le coordonnateur national de tout bien compromis.

*Chef/surintendant*

25) Le chef/surintendant est l'autorité portuaire déléguée pour les biens contrôlés, qui agit au nom du gestionnaire régional de la sécurité dans la région. Le chef/surintendant est responsable de tous les biens contrôlés se trouvant au port, et il :

- veille à ce que tous les responsables des biens respectent les politiques et les normes connexes sur les biens contrôlés;
- s'assure que tous les biens contrôlés sont entreposés en fonction des exigences en matière d'entreposage;
- veille à ce que tous les responsables des biens remplissent les formulaires BSF152, BSF208 et BSF203 au complet et fournissent tous les détails;
- s'assure que tous les transferts de biens sont documentés en conséquence et signalés au bureau régional de sécurité compétent;
- veille à ce que les nouveaux employés mutés au port signalent tous les biens contrôlés au bureau régional de sécurité respectif;
- se conforme aux vérifications et aux rapprochements lancés par le bureau régional de sécurité ou la SSM;
- avise le bureau régional de sécurité de tout bien de sécurité contrôlé compromis.

*Coordonnateur local*

26) Le coordonnateur local est la personne déléguée par le chef ou le surintendant et chargée de faire le contrôle de l'inventaire des biens contrôlés au port. Si le nom du coordonnateur local n'est pas fourni à la SSM, le chef ou le surintendant doit assumer ces fonctions. Le coordonnateur local :

- s'assure que les registres sont à jour et exacts;
- veille à ce que tous les inventaires des biens contrôlés sont entreposés en fonction des exigences en matière d'entreposage;







- se conforme aux vérifications et aux rapprochements lancés par le bureau régional de sécurité ou la SSM;
- s'assure que tous les formulaires de contrôle sont bien remplis, que les renseignements sont exacts et que tous les renseignements ont été fournis.

*Responsable des biens*

27) Le responsable des biens est tenu de respecter le code de conduite et les politiques sur les biens contrôlés, les politiques opérationnelles, les politiques de programme, les politiques sur l'uniforme et les normes connexes ainsi que la politique sur le signalement des incidents de sécurité. Le responsable des biens :

- remplit les formulaires de contrôle (BSF208, BSF203, BSF270 et BSF152);
- remplit les formulaires de contrôle en temps opportun et les présente au bureau régional de la sécurité une fois l'état du bien de sécurité contrôlé modifié;
- s'assure que tous les formulaires de contrôle sont exacts et dûment remplis avant leur présentation;
- veille à ce que le bien contrôlé soit entreposé conformément aux politiques et aux normes quand il a le bien en sa possession et au moment de verrouiller la salle;
- protège les renseignements et les biens dont il a la responsabilité, qu'il travaille sur place ou non, conformément aux règlements;[1]
- avise le bureau régional de sécurité de tout transfert et suit les directives fournies par l'agent de sécurité ou le spécialiste avant d'effectuer le transfert;
- continue à sensibiliser les gens aux questions et aux préoccupations en matière de biens contrôlés aux fins de la sécurité afin de s'assurer que leurs actions ne portent pas atteinte à la sécurité du ministère.[2]

**Demandes de renseignements**

28) Les demandes de renseignements doivent être adressées à la Direction de la sécurité et des normes professionnelles.

[1] 6.1.27 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579&section=text
[1] 6.1.30 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579&section=text

**Annexe A – Définitions**

[1] 6.1.27 http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578&section=text
[2] 6.1.30 http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578&section=text



Des définitions précises provenant de sources qui font autorité se trouvent dans le **Lexique de la terminologie en sécurité**.

**Formulaire de contrôle**

Les formulaires de contrôle servent à faire le suivi des déplacements des biens contrôlés ainsi que des incidents liés aux biens contrôlés aux fins de la sécurité.

BSF208 : Formulaire sur les biens contrôlés

BSF203 : Désignation du statut des échantillons d'impressions de timbres de point d'entrée

BSF152 : Rapport sur un incident relatif à la sécurité

BSF270 : Formulaire de départ ou de transfert d'un employé

BSF672 : Contrôle de l'utilisation quotidienne des timbres du point d'entrée.






Canada Border Services Agency Agence des services frontaliers du Canada



# Information Security Policy

Information Security

Infrastructure and Information Security Division

Security and Professional Standards Directorate

**27 January 2015**

PROTECTION • SERVICE • INTEGRITY





**Contents**











**EFFECTIVE DATE**

This policy is effective January 27, 2015.

**CONTEXT**

CBSA depends on information assets to deliver programs and services that are vital to the health, safety, security and economic well-being of Canadians. The information assets, as well as, any information assets entrusted to it by citizens, industry, municipal, provincial, territorial, foreign governments and other third parties (such as law enforcement agencies, security and intelligence organizations, etc.) must be appropriately safeguarded.

Information may occur in both physical and digital form: documents printed on paper, correspondence stored in a database, the dimensions of a precisely engineered piece of machinery, etc.

**APPLICATION**

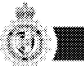
This policy is applicable to all CBSA management and employees (permanent, term, casual, part-time), contract and private agency personnel, and to individuals seconded or assigned to CBSA (including students).

This policy also applies to:

- All non-digital information assets (e.g. paper, microfilm);
- All digital information assets (e.g. diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks). This includes all devices which are leased, owned, purchased or otherwise used by the CBSA which have the capability to store/process CBSA information and may also include (but not limited to) such devices as multi-function devices, scanners, printers, photocopiers, etc.).);
- Mobile computing and communications devices with information storage capability (e.g. notebook/tablets/laptop computers, personal digital assistants, cellular phones, digital cameras and audio recording devices); and
- All situations where Classified, Protected and Sensitive information and/or assets are required to be removed from the workplace to employee residences, client premises or commercial accommodations and during transit on private or commercial modes of transportation (both electronic and otherwise).

The requirements of this information security policy equally apply to external service providers when they store or process CBSA information assets (e.g. Shared Service Canada, cloud computing services[1]).

[1] Cloud computing is a form of outsourcing information technology services and functions over the Internet.



**POLICY STATEMENT**

**OBJECTIVE**

The objective of this policy is to reduce the risk of loss and the unauthorized access to Classified, Protected and Sensitive information and/or assets under the care and control of CBSA and to:

- Promote a consistent approach to information security across the CBSA;
- Ensure consistency in the planning, operation, and monitoring of security activities;
- Provide a tool for the Departmental Security Officer (DSO) to inform CBSA users and management about the expected standard of behaviour and deal with misconduct or inappropriate behaviour; and
- Provide a foundation to help prevent, detect or mitigate activities that might result in an information security breach.

**EXPECTED RESULTS**

The expected results of this policy are to:

- Ensure that information security management is an identifiable and integral element of CBSA governance, programs, and services;
- Provide a common measure for improvements and compliance in protecting information and information resources;
- Ensure that information security policy instruments are adhered to and function as a source of good information security practices that should be common within the CBSA;
- Ensure that information security management activities at the CBSA do not increase risk to other departments or the government as a whole;
- Support the achievement and maintenance of an appropriate level of residual risk, suitable to the CBSA mandate, operations, priorities, and security requirements; and
- Provide a foundation for the correct reporting and timely investigations of security incidents.

Treasury Board Policy on Government Security http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text

Values and Ethics Code for the Public Sector http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25049

**REQUIREMENTS**

The CBSA must:

- Protect the confidentiality, integrity and availability of the information assets in its care;
- Ensure that information assets are identified and categorized based on the degree of potential injury (national interests or non-national interests) that could result if compromised;







- Restrict access to information assets to authorized individuals using security measures outlined in this policy and underlying standards;
- Ensure that information assets must be securely stored when not in use or when left unattended in accordance with the classification level of the information or asset(s);
- Ensure that Classified, Protected and Sensitive information and/or assets are adequately safeguarded during storage, transport and use outside the workplace;
- Ensure that Classified, Protected and Sensitive information and/or assets are disposed of appropriately in accordance with the level of sensitivity of the information or asset(s); and
- For Protected B and above information assets:
  - Employ automated mechanisms to restrict access to information assets storage areas and audit access attempts and access granted.
  - Use cryptographic mechanisms to protect and restrict access to information on portable digital media.

**Need to Know Principle**

Notwithstanding any security identification and categorization, access to sensitive information and sensitive assets must be limited to individuals who have been security screened to a level equal to, or above the level of the information or asset and whose duties require access to the information or asset. Personnel are not entitled to access merely for convenience or because of status, rank, office or level of clearance.

The need-to-know principle must be applied in all aspects of security including, but not limited to:

- Determining to whom the information or assets may be distributed; and
- The marking of information assets to identify who may have access
- Third parties with whom the CBSA shares information

**Information Sharing**

The CBSA Departmental Security Officer is responsible for ensuring that agreements and memorandums of understanding are established, monitored and periodically reviewed (with respect to security controls/agreements) when sharing information with other government departments, provincial and territorial governments, external organizations and foreign governments, in compliance with applicable legislation, international agreements and arrangements and Treasury Board Secretariat policies, directives and standards for the appropriate safeguarding of information and sensitive assets prior to distribution.

Information sharing agreements or memorandums of understanding must include the following:







- A description of the types of information to be shared;
- The purpose for which the information is being shared;
- A stipulation that the information is to be distributed only on a need-to-know basis within the recipient department, organization or government;
- The conditions for disclosing information to third parties; and
- The name, title and signature of the appropriate officials in both the originating department, organization or government and the receiving department, organization or government and the period covered by the agreement or arrangement.

**Distribution**

Prior to distribution of information assets, managers must ensure that:

- Information assets are categorized at the appropriate level and marked in accordance with departmental marking and categorization guidelines;
- Any requirement for declassification or downgrading of information assets are identified;
- Any requirement for additional markings, such as caveats or dissemination markings are identified;
- Authorization from the originator of the information or asset is obtained before third party sharing is permitted; and
- All arrangements and memorandums of understanding involving the exchange of personal information meet the requirements of the *Access to Information and Privacy Acts*. For more detailed/specific references and guidance, please refer to the Acts themselves or contact the Access to Information and Privacy organization within the CBSA.

Access to Information Act http://laws-lois.justice.gc.ca/eng/acts/A-1/

Policy on the Disclosure of Customs information http://atlas/cab-dgsi/res/toolkit-outils/partnership-partenariat/is-ei/section107-article107/107_eng.asp

Introduction to the Privacy Act http://atlas/csd-dsg/toolkit-outils/atip-aiprp/reference/04_eng.asp

**ROLES, RESPONSIBILITIES AND ACCOUNTABILITY**

**Information Assets Authors**

Information assets authors are responsible for:

- Identifying and categorizing information assets that they create or collect;
- Marking information assets with the appropriate level;
- Declassifying or downgrading information assets when safeguards appropriate to the identified category are no longer required; and
- Pay special attention to personal information collected as it requires protection throughout its life cycle such as, but not limited to, interviews, reports, application forms, and questionnaires.







**Managers at all levels**

Managers at all levels are responsible for:

- Ensuring that all information, created or collected within their area of responsibility, is identified, categorized, and marked with the appropriate level;
- Ensuring that all information is declassified or downgraded once safeguards appropriate to the identified category are no longer required;
- Ensuring that employees have the appropriate personnel security screening level and the need to know prior to allowing them access to Classified or Protected information or assets; and
- Procuring external services to process and store CBSA information (e.g. Shared Services Canada, Cloud computing) must ensure that service agreements with these external service providers meet the requirements of this information security policy.

**CBSA Employees**

CBSA employees are responsible for:

- Keeping themselves informed where possible of any and all requirements they are responsible for in order to uphold security integrity at the CBSA
- Appropriately storing, handling and disposing or sanitizing all information assets in their care.

**COMPLIANCE AND REPORTING**

The CBSA Departmental Security Officer, security practitioners and managers are responsible for monitoring compliance with this policy within the CBSA, measuring the effectiveness of identification, security categorization and marking of information resources and ensuring appropriate remedial actions are taken when deficiencies arise.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Volume, Reporting of Security Incidents.

**CONSEQUENCES**

The DSO is responsible for investigating and responding to reports of non-compliance with this policy and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies; directives or standards may be subject to a review and possibly a revocation of the CBSA Reliability Status, disciplinary action, up to and including termination of employment.







## POLICY REVIEW

The DSO (Director General, Security and Professional Standards Directorate) should initiate a review of this policy once every three years, or earlier as required.

## REFERENCES

**Laws and Regulations**

- Canadian Charter of Rights and Freedoms - http://laws-lois.justice.gc.ca/eng/const/page-15.html
- Canadian Human Rights Act - http://laws-lois.justice.gc.ca/eng/acts/h-6/
- Privacy Act - http://laws-lois.justice.gc.ca/eng/acts/P-21/
- Personal Information Protection and Electronic Documents Act - http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

**Treasury Board Secretariat**

- TBS Policy on Government Security - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578
- TBS Policy on Privacy Protection - https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text
- TBS Policy on Information Management - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742
- TBS Directive on Departmental Security Management - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579
- TBS Operational Security Standard on Physical Security - https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329&section=text
- Security Organization and Administration Standard of the PGS; http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=12333&section=text
- Values and Ethics Code for the Public Sector - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=25049

**Royal Canadian Mounted Police**

- RCMP Guide G1-001, Security Equipment Guide - http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm
- RCMP Guide G1-009, Transport and Transmittal of Protected and Classified Information - http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-eng.htm

**Communications Security Establishment Canada**

- CSEC Directive ITSD-03 Directive for the Control of COMSEC Material in the Government of Canada - https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsd03a-eng_1.pdf





- CSEC Guidance ITSG-33 Annex 1 IT Security Risk Management: A Lifecycle Approach – Departmental IT Security Risk Management Activities - https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg33-ann1-eng_0.pdf
- CSEC Guidance ITSG-33 Annex 2 IT Security Risk Management: A Lifecycle Approach – Information System Security Risk Management Activities - https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg33-ann2-eng_1.pdf
- CSEC Guidance ITSG-06 Clearing and Declassifying Electronic Data Storage Devices - https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg06-eng.pdf

**Canada Border Services Agency**

- Use of Force Equipment Policy
- Customs Directive D19-13-2
- Uniform Handbook

**ENQUIRIES**

Enquiries regarding this policy should be directed to:

**Security and Professional Standards Directorate**

E-mail: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Intranet : http://atlas/cb-dgc/sec/index_e.asp


Agence des services frontaliers du Canada | Canada Border Services Agency



# Politique sur la sécurité de l'information

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

**Le 27 janvier 201**

PROTECTION • SERVICE • INTÉGRITÉ





Table des matières











DATE D'ENTRÉE EN VIGUEUR

La politique entre en vigueur le 27 janvier 2015.

CONTEXTE

L'Agence des services frontaliers du Canada (ASFC) s'appuie sur des ressources d'information pour offrir des programmes et services qui sont essentiels à la santé, à la sûreté, à la sécurité et au bien-être économique des Canadiens. Les ressources d'information de l'ASFC, ainsi que toutes les ressources d'information qui sont confiées à celle-ci par les citoyens, l'industrie, les administrations municipales, les gouvernements provinciaux, territoriaux, les gouvernements étrangers et les autres tiers (tel que les autorités policières, organisations de sécurité et de renseignements, etc.), doivent être protégées de façon appropriée.

L'information pouvant exister à la fois sur support matériel et sur support numérique (documents imprimés sur du papier, pièces de correspondance stockées dans une base de données, dimensions d'une pièce d'équipement conçue avec précision, etc.)

APPLICATION

La présente politique s'applique à tous les gestionnaires et employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), aux contractuels et aux employés des agences privées ainsi qu'aux personnes en détachement ou affectées à l'ASFC (y compris les étudiants).

La politique s'applique à :

- toutes les ressources d'information non numériques (p. ex. papier, microfilm);
- toutes les ressources d'information numériques (p. ex. disquettes, bandes magnétiques, disques durs externes ou amovibles, clés USB, disques compacts, vidéodisques numériques). Ceci comprend tous les appareils loués, achetés, appartenant à l'Agence, ou par ailleurs utilisés à l'Agence, qui permettent de stocker et de traiter des données de l'ASFC, et peut aussi comprendre notamment des appareils multifonctions tels que des scanneurs, des imprimantes, des photocopieurs, etc.;
- tous les appareils informatiques et de communication mobiles ayant une capacité de stockage d'information (p. ex. blocs-notes/ordinateurs portatifs, assistants numériques, téléphones cellulaires, appareils photo numériques et appareils d'enregistrement);
- toutes les situations où des renseignements ou des biens classifiés, protégés et de nature délicate doivent être déplacés du lieu de travail à la résidence d'un employé, aux locaux d'un client ou vers des installations commerciales, et ce, que le mode de transport (numérique ou autre) soit privé ou commercial.







Les exigences de cette politique sur la sécurité de l'information s'appliquent tout autant aux fournisseurs de services externes lorsqu'ils stockent ou traitent des ressources d'information de l'ASFC (p. ex. Services partagés Canada, services d'informatique en nuage[1]).

**ÉNONCÉ DE LA POLITIQUE**

**OBJECTIF**

L'objectif de la politique consiste à réduire le risque de perte de renseignements et de biens classifiés, protégés et de nature délicate sous le contrôle et la garde de l'ASFC et l'accès non autorisé à ces derniers, et à:

- favoriser une approche uniforme en matière de sécurité de l'information à l'échelle de l'ASFC;
- garantir l'uniformité dans la planification, la tenue et la surveillance des activités de sécurité;
- fournir à l'agent de sécurité du ministère (ASM) un outil lui permettant de renseigner les utilisateurs et de la gestion de l'ASFC sur les normes de conduite attendues ainsi que d'intervenir dans les cas d'inconduite ou de comportement inapproprié; et
- donner des outils de base pour la prévention, la détection ou l'atténuation des activités susceptibles de mettre en péril la sécurité de l'information.

**RÉSULTATS ESCOMPTÉS**

Les résultats escomptés de la présente politique sont comme suit :

- Veiller à ce que la gestion de la sécurité de l'information soit un élément identifiable et constitue une partie intégrante de la gouvernance, des programmes et des services de l'ASFC;
- Établir une mesure commune en vue de l'apport d'améliorations et de la surveillance de la conformité en ce qui touche la protection des renseignements et des ressources d'information;
- Voir à ce que les instruments de politique liés à la sécurité de l'information soient respectés et utilisés comme source de pratiques exemplaires en matière de sécurité de l'information au sein de l'ASFC;
- Veiller à ce que les activités de gestion de la sécurité de l'information à l'ASFC n'augmentent pas les risques courus par les autres ministères ou par l'ensemble du gouvernement;
- Soutenir l'atteinte et le maintien d'un niveau de risque résiduel acceptable par rapport au mandat, aux opérations, aux priorités et aux exigences en matière de sécurité de l'ASFC; et
- Fournir des outils de base pour le signalement approprié des incidents de sécurité, et les enquêtes sur ceux-ci au moment opportun.

[1] L'informatique en nuage est une forme d'impartition des services qui fonctionne par l'intermédiaire d'Internet.



Politique sur la sécurité du gouvernement du Secrétariat du Conseil du Trésor du Canada : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578&section=text

Code de valeurs et d'éthique du secteur public du Secrétariat du Conseil du Trésor du Canada : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=25049

**EXIGENCES**

L'ASFC doit :

- Protéger la confidentialité, l'intégrité et la disponibilité des ressources d'information en sa possession;
- Voir à ce que les ressources d'information soient identifiées et catégorisées selon le degré des dommages potentiels (intérêts nationaux ou non nationaux) qui pourraient résulter de leur compromission;
- Limiter l'accès aux ressources d'information aux personnes autorisées, au moyen des mesures de sécurité décrites dans la politique et des normes sous-jacentes;
- Veiller à ce que les ressources d'information soient stockées de façon sécuritaire lorsqu'elles ne sont pas utilisées ou quand elles sont sans surveillance, conformément au niveau de classification des renseignements ou des biens;
- Voir à ce que les renseignements et les biens classifiés, protégés et de nature délicate soient protégés adéquatement pendant leur entreposage, leur transport et leur utilisation à l'extérieur du lieu de travail;
- Veiller à ce que les renseignements et les biens classifiés, protégés et de nature délicate soient éliminés de façon appropriée, en fonction de leur caractère délicat; et
- Pour ce qui est des ressources d'information de niveau « Protégé B » ou supérieur :
    - Utiliser des mécanismes automatisés pour restreindre l'accès aux zones de stockage des ressources d'information et pour détecter les tentatives d'accès et les accès accordés.
    - Utiliser des mécanismes cryptographiques pour protéger l'information stockée dans des supports numériques portatifs et limiter l'accès à celle-ci.







### Principe du besoin de connaître

Indépendamment de toute désignation ou classification de sécurité, l'accès aux renseignements de nature délicate doit être limité aux personnes qui détiennent une cote de sécurité de niveau égal ou supérieur à celui des renseignements ou des biens, et dont les fonctions nécessitent l'accès aux renseignements ou aux biens. Il ne faut pas que les employés aient accès aux renseignements simplement pour des raisons pratiques ou parce que leur statut, leur grade, leur poste ou leur niveau d'autorisation leur permettent un tel accès.

Le principe du besoin de connaître doit être appliqué à tous les aspects de la sécurité, dont les suivants :

- Déterminer à qui les renseignements ou les biens peuvent être fournis,
- Marquer les ressources d'information en y indiquant les intervenants qui peuvent y avoir accès.
- Les tiers avec qui l'ASFC échange les renseignements

### Échange de renseignements

L'agent de sécurité du ministère de l'ASFC doit veiller à ce que des accords et des protocoles d'entente soient établis, surveillés et examinés périodiquement (en ce qui a trait aux contrôles et aux ententes de sécurité) lorsqu'il échange des renseignements avec d'autres ministères, des gouvernements provinciaux et territoriaux, des organismes externes et des gouvernements étrangers, conformément aux lois, aux ententes et aux arrangements internationaux applicables, ainsi qu'aux politiques, directives et normes du Secrétariat du Conseil du Trésor concernant la protection appropriée des renseignements et des biens de nature délicate avant leur distribution.

Les accords ou les protocoles d'entente sur l'échange de renseignements doivent renfermer ce qui suit :

- Une description des types de renseignements à échanger.
- Les raisons pour lesquelles les renseignements sont communiqués.
- Une stipulation selon laquelle ces renseignements ne doivent être transmis qu'aux personnes qui ont besoin de les connaître au sein du ministère, de l'organisation ou du gouvernement destinataire.
- Les conditions de la communication des renseignements à des tiers.
- Les noms, titres et signatures des fonctionnaires compétents du ministère, de l'organisation ou du gouvernement d'origine, ainsi que du ministère, de l'organisation ou du gouvernement destinataire, ainsi que la durée précise de l'entente.







### Distribution

Avant de distribuer des ressources d'information, les gestionnaires doivent veiller à ce que :

- les ressources d'information soient catégorisées au niveau approprié et marquées conformément aux lignes directrices en matière de marquage et de catégorisation de l'Agence;
- toute exigence liée à la déclassification ou au déclassement de ressources d'information soit identifiée;
- toute exigence liée à des mentions additionnelles, comme des mises en garde ou des mentions concernant la diffusion, soit identifiée;
- l'autorisation de l'auteur des renseignements ou du bien soit obtenue avant que l'échange avec un tiers soit permis;
- tous les arrangements et les protocoles d'entente régissant l'échange de renseignements personnels satisfassent aux exigences de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. Pour obtenir des renseignements plus détaillés ou des références précises et plus de consignes, veuillez consultez les lois ou communiquer avec le Bureau de l'Accès à l'information et protection des renseignements personnels (AIPRP) de l'ASFC.

Loi sur l'accès à l'information : http://laws-lois.justice.gc.ca/fra/lois/A-1/

Politique sur la divulgation des renseignements douaniers : http://atlas/cab-dgsi/res/toolkit-outils/partnership-partenariat/is-ei/section107-article107/107_fra.asp

Introduction à la Loi sur la protection des renseignements personnels : http://atlas/csd-dsg/toolkit-outils/atip-aiprp/reference/04_fra.asp

## RÔLES, RESPONSABILITÉS ET RESPONSABILISATION

### Auteurs des ressources d'information

Responsabilités des auteurs des ressources d'information :

- Identifier et catégoriser les ressources d'information qu'ils créent ou recueillent.
- Marquer les ressources d'information au niveau approprié.
- Déclassifier ou déclasser les ressources d'information lorsque les mesures de protection appropriées pour la catégorie attribuée ne sont plus requises.







- Porter une attention particulière aux renseignements personnels recueillis (p. ex. entrevues, rapports, formulaires de demande et questionnaires), car ils doivent être protégés tout au long de leur cycle de vie.

**Gestionnaires de tous les niveaux**

Responsabilités des gestionnaires de tous les niveaux :

- Veiller à ce que toutes les informations créées ou recueillies dans leur secteur de responsabilité soient identifiées, catégorisées et marquées au niveau approprié;
- Veiller à ce que tous les renseignements soient déclassifiés ou déclassés une fois que les mesures de protection appropriées pour la catégorie attribuée ne sont plus requises;
- Veiller à ce que les employés fassent l'objet du niveau d'enquête de sécurité sur le personnel approprié et qu'ils aient besoin de connaître les renseignements avant de leur donner accès à des renseignements ou à des biens protégés ou classifiés; et
- Faire appel à des fournisseurs de services externes pour traiter et stocker l'information de l'ASFC (p. ex. Services partagés Canada, services d'informatique en nuage), et veiller à ce que les ententes de service conclues avec ces fournisseurs satisfassent aux exigences de cette politique sur la sécurité de l'information.

**Employés de l'ASFC**

Responsabilités des employés de l'ASFC :

- De se tenir informés si possible de tout et de toutes les exigences de ce qu'ils sont responsables afin de préserver l'intégrité de la sécurité à l'ASFC
- Stocker, manipuler, et éliminer ou nettoyer de façon appropriée les ressources d'information en leur possession.

**CONFORMITÉ ET RAPPORTS**

L'agent de sécurité du ministère, les spécialistes de la sécurité et les gestionnaires de l'ASFC doivent surveiller la conformité à cette politique au sein de l'ASFC, mesurer l'efficacité de l'identification, de la catégorisation de sécurité et du marquage des ressources d'information, et veiller à ce que les mesures correctives appropriées soient prises lorsque des lacunes sont relevées.

Les employés signaleront les incidents de sécurité conformément aux exigences décrites dans le Volume de sécurité de l'ASFC, Signalement des incidents de sécurité.







## CONSÉQUENCES

L'agent de sécurité du ministère doit enquêter et intervenir lorsque des cas de non-conformité à la politique sont signalés, et voir à ce que les mesures correctives appropriées soient prises au moment opportun, s'il y a lieu. Toute violation des politiques, des directives ou des normes par un employé peut entraîner des mesures disciplinaires pouvant aller jusqu'au renvoi.

## EXAMEN DE LA POLITIQUE

L'agent de sécurité du ministère (directeur général, Direction de la sécurité et des normes professionnelles) doit examiner la politique au moins une fois à tous les trois ans, ou à un intervalle plus court s'il le juge nécessaire.

## RÉFÉRENCES

### Lois et règlements

- *Charte canadienne des droits et libertés* - http://laws-lois.justice.gc.ca/fra/const/page-15.html
- *Loi canadienne sur les droits de la personne* - http://laws-lois.justice.gc.ca/fra/lois/h-6/
- *Loi sur la protection des renseignements personnels* - http://laws-lois.justice.gc.ca/fra/lois/P-21/
- *Loi sur la protection des renseignements personnels et les documents électroniques* - http://laws-lois.justice.gc.ca/fra/lois/P-8.6/index.html

### Secrétariat du Conseil du Trésor

- Politique sur la sécurité du gouvernement - http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=16578
- Politique sur la protection de la vie privée - https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510&section=text
- Politique sur la gestion de l'information - http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12742
- Directive sur la gestion de la sécurité ministérielle - http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16579
- Norme opérationnelle sur la sécurité matérielle - https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329&section=text
- Norme de sécurité relative à l'organisation et l'administration de la Politique sur la sécurité du gouvernement - http://tbs-sct.gc.ca/pol/doc-fra.aspx?id=12333&section=text
- *Code de valeurs et d'éthique du secteur public* - http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=25049







**Gendarmerie royale du Canada**

- G1-001 - Guide d'équipement de sécurité - http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm
- G1-009 - Transport et transmission de renseignements protégés ou classifiés - http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-fra.htm

**Centre de la sécurité des télécommunications Canada**

- Directive en matière de sécurité TI (ITSD) ITSD-03 : Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein du gouvernement du Canada - https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsd03a-fra.pdf
- Orientation sur la sécurité des technologies de l'information (ITSG) ITSG-33 (annexe 1) : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des TI – https://www.cse-cst.gc.ca/fr/learning-formation/course-cours/gestion-risques-lies-a-securite-ti-methode-axee-cycle-vie-itsg-33
- ITSG-33 (annexe 2) : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des systèmes d'information - https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsg33-ann2-fra_1.pdf
- ITSG-06 : Effacement et déclassification des supports d'information électroniques – https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsg06-fra.pdf

**Agence des services frontaliers du Canada**

- Politique concernant le matériel utilisé en cas de recours à la force
- Mémorandum D19-13-2
- Guide des uniformes

**DEMANDES DE RENSEIGNEMENTS**

Pour toute demande de renseignements concernant la présente politique, veuillez communiquer avec :

| **Direction de la sécurité et des normes professionnelles** |
|---|
| Courriel : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca |
| Intranet : http://atlas/cb-dgc/sec/index_f.asp |

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for Classification of Information Assets

Information Security

Infrastructure and Information Security Division

Security and Professional Standards Directorate

27 January 2015

PROTECTION • SERVICE • INTEGRITY





Contents



# EFFECTIVE DATE

This standard is effective January 27, 2015.

# CONTEXT

Identification, categorization and marking of information and assets are an integral part of the planning, design and delivery of government programs and services and are the first step in protecting that information. Once it is known where information is located and what level of classification applies, appropriate safeguards can be applied.

# APPLICATION

This standard is applicable to all CBSA management and employees (permanent, term, casual, part-time), contract and private agency personnel, and to individuals seconded or assigned to CBSA (including students).

# STANDARD STATEMENT

## OBJECTIVE

The objective of this standard is to ensure that all CBSA information and assets are consistently and correctly identified, categorized and marked at the appropriate level in order to optimally use departmental resources in their processing and safekeeping.

## EXPECTED RESULTS

The expected results of this standard are to:

- Optimally use departmental resources in the processing and safekeeping of information assets;
- Enable CBSA resources to apply security controls where protected/sensitive information is to be processed, stored and/or transmitted on the CBSA Information Technology (IT) computer systems;
- Maintain an adequate classification of information assets throughout their lifecycle.

# REQUIREMENTS

CBSA must:







- Identify, categorize and mark information assets according to their confidentiality, integrity and availability[1];
- Mark removable media indicating applicable security markings (such as date, owner, classification, etc.) (if any);
- Maintain identification, categorization and marking of information assets throughout their information life cycle (Note: including the declassifying/downgrading of information sensitivity) to reflect changes in requirements for confidentiality, integrity or availability.

## COMPLIANCE AND REPORTING

The CBSA Departmental Security Officer (DSO), security practitioners and managers are responsible for monitoring compliance with this standard within CBSA, measuring the effectiveness of identification, security categorization and marking of information resources and ensuring appropriate remedial actions are taken when deficiencies arise.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Volume, Reporting of Security Incidents.

## CONSEQUENCES

The DSO (Departmental Security Officer) is responsible for investigating and responding to reports of non-compliance with this standard and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies, directives or standards may be subject to a review and possibly a revocation of the CBSA Reliability Status, disciplinary action, up to and including termination of employment.

## STANDARD REVIEW

The DSO (Director General Security and Professional Standards Directorate) should initiate a review of this standard at a minimum of every three years, or earlier, as required.

## REFERENCES

- CSEC ITSG-33 Annex 1 *IT Security Risk Management: A Lifecycle Approach – Departmental IT Security Risk Management Activities*

[1] For detailed information, see Procedures for Identification, Categorization and Marking of Information Assets.





- *CSEC ITSG-33 Annex 2 IT Security Risk Management: A Lifecycle Approach – Information System Security Risk Management Activities*

- CBSA Online guide for classification of information

# INQUIRIES

Inquiries regarding this standard should be directed to:

**Security and Professional Standards Directorate**
E-mail: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca
Intranet : http://atlas/cb-dgc/sec/index_e.asp

# DEFINITIONS

Definitions related to this standard are included in the Glossary of Security Terminology.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme de classification des ressources d'information

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

Le 27 janvier 2015

PROTECTION • SERVICE • INTÉGRITÉ





Agence des services frontaliers du Canada | Canada Border Services Agency



PROTECTION • SERVICE • INTÉGRITÉ

Canadä



## Table des matières









# DATE D'ENTRÉE EN VIGUEUR

La présente norme entre en vigueur le 27 janvier 2015.

# CONTEXTE

L'identification, la catégorisation et le marquage des renseignements et des biens font partie intégrante de la planification, de la conception et de la prestation des programmes et des services du gouvernement et constituent la première étape en vue de la protection de ces renseignements. Une fois que l'on connaît l'emplacement et le niveau de classification des renseignements, les mesures de protection appropriées peuvent être appliquées.

# APPLICATION

La présente norme s'applique à tous les gestionnaires et employés de l'Agence des services frontaliers du Canada (ASFC) (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), aux contractuels et aux employés des agences privées ainsi qu'aux personnes en détachement ou affectées à l'ASFC (y compris les étudiants).

# ÉNONCÉ DE LA NORME

## OBJECTIF

La présente norme a pour objectif de veiller à ce que tous les renseignements et les biens de l'ASFC soient identifiés, catégorisés et marqués de façon uniforme, exacte et au niveau approprié afin d'être en mesure d'utiliser de façon optimale les ressources de l'Agence dans le cadre du traitement et de la protection de ces renseignements.







## RÉSULTATS ESCOMPTÉS

Les résultats escomptés de la présente norme sont les suivants :

- Utiliser de façon optimale les ressources de l'Agence dans le cadre du traitement et de la protection des ressources d'information;
- Permettre aux ressources de l'ASFC d'appliquer des contrôles de sécurité dans les cas où les renseignements protégés et de nature délicate doivent être traités, stockés et/ou communiqués sur les systèmes informatiques de technologie de l'information (TI) de l'ASFC;
- Maintenir une classification adéquate des ressources d'information tout au long de leur cycle de vie.

# EXIGENCES

L'ASFC doit :

- Identifier, catégoriser et marquer les ressources d'information en fonction de leur confidentialité, intégrité et disponibilité[1];
- Marquer les supports amovibles en indiquant les marquages de sécurité applicables (comme la date, le propriétaire, la classification, etc.) [le cas échéant];
- Tenir à jour l'identification, la catégorisation et le marquage des ressources d'information tout au long de leur cycle de vie (incluant les cas où l'on réduit la cote faisant part de la nature délicate des renseignements en cause, ou encore lorsque l'on enlève toute cote attribuée en ce sens) afin de refléter les changements apportés aux exigences de confidentialité, d'intégrité et de disponibilité.

# CONFORMITÉ ET RAPPORTS

L'agent de sécurité du ministère, les spécialistes de la sécurité et les gestionnaires de l'ASFC doivent surveiller la conformité à cette norme au sein de l'ASFC, mesurer l'efficacité de l'identification, de la catégorisation de sécurité et du marquage des ressources d'information, et veiller à ce que les mesures correctives appropriées soient prises lorsque des lacunes sont relevées.

Les employés signaleront les incidents de sécurité conformément aux exigences décrites dans le Volume de sécurité de l'ASFC, Signalement des incidents de sécurité.

---

[1] Pour de plus amples renseignements, consultez les Procédures d'identification, de catégorisation et de marquage des ressources d'information.







# CONSÉQUENCES

L'agent de sécurité du ministère doit enquêter et intervenir lorsque des cas de non-conformité à la norme sont signalés, et voir à ce que les mesures correctives appropriées soient prises au moment opportun, s'il y a lieu. Toute violation des politiques, des directives ou des normes par un employé peut entraîner des mesures disciplinaires pouvant aller jusqu'au renvoi.

# EXAMEN DE LA NORME

L'agent de sécurité du ministère (directeur général, Direction de la sécurité et des normes professionnelles) devrait réaliser un examen de la norme tous les trois ans, ou à un intervalle plus court s'il le juge nécessaire.

# RÉFÉRENCES

- ITSG-33 Annexe 1 *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des TI* du Centre de la sécurité des télécommunications Canada (CSTC)
- ITSG-33 *Annexe 2 La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des systèmes d'information* du CSTC
- Guide en ligne pour la classification de l'information de l'ASFC

# DEMANDES DE RENSEIGNEMENTS

Pour toute demande de renseignements concernant la présente norme, veuillez communiquer avec :

**Direction de la sécurité et des normes professionnelles**

Courriel : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Intranet : http://atlas/cb-dgc/sec/index_f.asp





# DÉFINITIONS

Les définitions relatives à la présente norme figurent  dans le Lexique de terminologie de la sécurité.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Procedures for Identification, Categorization and Marking of Information Assets

Information Security

Infrastructure and Information Security Division

Security and Professional Standards Directorate

27 January 2015

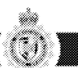
PROTECTION • SERVICE • INTEGRITY








# Contents



## Objective

The following procedures are intended to highlight the responsibilities of authors and/or recipients to properly identify information or assets.

## Identify Key Categories

All information held by the CBSA that requires safeguarding falls under two key categories depending on whether a possible injury deriving from the compromise of information assets would affect the following interests:

1. National Interests

   National interest refers to information and assets concerning the security and social political and economic stability of Canada.

2. Non-National Interests

   Non-National interest refers to information and assets concerning interest other than the national interest, including individuals, government institutions and businesses, such as personal information, law enforcement information and competitive information such as trade secrets, third party information, etc.

## Categorization

Any author/owner of information for the CBSA must perform an injury test to determine the categorization level of the information/asset. If the information or asset has been determined as being sensitive to either a non-national interest (protected) or to a national interest (Classified), the following injury test must be performed to determine the degree of potential injury. Should assistance be required, please contact Information Security within the Security and Professional Standards Diretorate.

In order to apply the injury test, an evaluation of the severity of the likely injury which would result if the confidentiality, integrity or availability of an informational asset would be compromised. If the potential harm would be to the National interest then the appropriate category based on the magnitude of the injury would be selected from the Confidential, Secret, or Top Secret categories. If the potential harm would be to the non-national interest then the appropriate category, based on the magnitude of the injury, would be selected from the Protected A, B or C categories.

In conducting the injury test, in no case should information or assets be categorized in such a way as to:

- Hide violations of the law, inefficiency or conceal administrative error.







- Prevent embarrassment to a department, organization or official.
- Restrain competition.
- Prevent or delay the release of information that does not require protection in the public interest.

The first step is to determine if the information or asset under the care of the CBSA is **protected, classified,** or **unclassified** at the time it is created or collected based on one of the two Key categories (non-national or national interests, as noted above).

**Protected information assets**
Information and assets are considered **protected** if compromise could cause injury to a non-national interest, such as a traveller, an employee or the CBSA mandate. Some examples (not limited to) of what may be considered protected are listed below:

- Employee personal information (sufficient combination of personal information);
- Third party information (business, financial, commercial, scientific, research and technical information received from, pertaining to or affecting third parties);
- Legal proceedings and/or law enforcement (linked to the application of the *Customs Act* or internal to the CBSA);
- Government research;
- Investigations (including techniques, plans);
- Discussions regarding potential negotiated settlements (including exchange of views between employees);
- Recording of discussions on operational issues (such as internal decision-making process/operations that could cause damage to aforementioned process); and
- Vulnerability of particular buildings or other structures or systems, including computer or communication systems, or methods employed to protect such buildings or other structures or systems.

Protected information assets are divided into three levels of categorization depending on the potential level of injury to the Non-National interest, such as individuals, businesses or government institutions

Categorization - If unauthorized disclosure could reasonably be expected to cause…

| | |
|---|---|
| PROTECTED C | Extremely grave injury to a non-national interest. This category of information, considered extremely sensitive, applies to a very limited amount of information with a high degree of potential injury. For example, the name of an informant in a criminal investigation or other information concerning safety of individuals or law enforcement, if compromised, could mean loss of life. |
| PROTECTED B | Serious injury to a non-national interest. This category of information, considered *particularly sensitive*, exists both in large quantities and in large concentrations within the CBSA. If compromised, there is a medium degree of potential injury to a citizen, or an organization, such as identity theft or the loss of a competitive advantage. This medium degree of potential injury can also mean 'lasting harm or embarrassment' that |



could have direct negative effects on an individual's career, reputation, financial position, safety, health or well-being.

Information can also fit into the Protected B category due to its nature, for example: investigations into violations of law (Special Investigations cases), solicitor-client privilege, and scientific research material submitted to the CBSA.

PROTECTED A — Injury to a non-national interest. This category includes *low-sensitive* or personal information of a routine nature, for example, an exact salary figure, which if compromised, could cause a low degree of injury or embarrassment to an individual or an organization.

**Classified**

Information and assets are considered **classified**, if disclosed, modified, distributed or destroyed could cause injury to a national interest, such as the defence and maintenance of social, political, and economic stability of Canada. Some examples (not limited to) of what may be considered classified are listed below:

- Federal/Provincial Affairs ;
- International Affairs (such as information obtained in confidence from a foreign government);
- Defence of Canada (including any state allied or associated with Canada)
- Economic interests of Canada, including trade secrets or financial, commercial, scientific or technical information that belongs to the Government of Canada or a government institution and has substantial value or is reasonably likely to have substantial value;
- Law enforcement and investigations (such as activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*); and
- Confidences of Queen's Privy Council.

Categorization — If unauthorized disclosure could reasonably be expected to cause…

TOP SECRET — Exceptionally grave injury to the national interest. Information concerning potential armed hostilities toward Canada or its allies could reasonably be expected to cause exceptionally grave injury to the national interest if compromised, and would therefore be classified at **Top secret level**.

SECRET — Serious injury to the national interest. Submissions for legislative amendments or details of important international negotiations warrant categorization at the **Secret level**.





CONFIDENTIAL — Injury to the national interest. Information classified at the **Confidential level**, such as strategy papers on intelligence operations and targeting information, or of discussions of federal interdepartmental committees could reasonably be expected to cause injury to the national interest if compromised.

**Unclassified (not protected or classified)**
If the information or asset does not fall into either the protected or classified categories, it is considered non-sensitive and no particular security measures apply.

Note: Information that is publicly available may not be categorized as protected or classified (however, there may be instances where such things as open source material on government activities is not classified in the public domain, but once the Government acknowledges/recognizes it, then it will have some sensitivity/classification placed upon it i.e. Insider threat on public information).

- Information that is published or available for purchase by the public.
- Information that is posted on the CBSA Internet Web site.
- Information that is kept in the CBSA public locations.
- Information that has already been disclosed under the *Access to Information Act* by the appropriate authority within the CBSA.

An "**Unclassified" designation** refers to information and assets that pose no potential injury to the national interest or non-national interest if disclosed, modified, distributed or destroyed. The categorization of unclassified is not synonymous with making it publicly available nor does it remove the need-to-know component. Normal access to information processes still apply.

Any information or asset that does not contain a categorization marking indicates it has not been assessed through an injury test and may be treated as unclassified.

**Other Specialized Categories**

Confidences of the Queen's Privy Council (Cabinet Confidences) is a specialized category whose definition and treatment is described in the Privy Council Office Policy on the Security of Cabinet Confidences (2014).

APPENDIX

| PROTECTED Information | NON-NATIONAL Interest |
|---|---|
| PROTECTED A: Information whose compromise could reasonably be expected to cause injury to non-national interests (e.g. routine complaints, general information). | Reliability Status (RS) – this is a security level and a prerequisite to a Secret or Top Secret clearance. |
| PROTECTED B: Information applies to particularly sensitive information or other assets whose compromise could reasonably be expected to cause serious injury to non-national interests (e.g. medical descriptions, organized crime). | |
| PROTECTED C: Extremely sensitive information or other assets whose compromise could reasonably be expected to cause extremely grave injury to non-national interests (e.g. information concerning life threatening situations). | |
| **CLASSIFIED Information** | **NATIONAL Interest** |
| CONFIDENTIAL / SECRET: Information whose unauthorized disclosure could reasonably be expected to cause serious injury to the national interest. | Security Clearance – Secret |
| TOP SECRET: Information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave injury to the national interest. | Security Clearance – Top Secret<br><br>One may also be Top Secret with Indoctrination base on their functions. |


Agence des services frontaliers du Canada | Canada Border Services Agency



# Procédures d'identification, de catégorisation et de marquage des ressources d'information

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

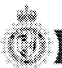
Le 27 janvier 2015

PROTECTION • SERVICE • INTÉGRITÉ





# Table des matières



# Objectif

Les procédures suivantes visent à préciser les responsabilités des auteurs et/ou des destinataires afin d'identifier adéquatement les renseignements ou les biens.

# Description des principales catégories

Tous les renseignements que détient l'Agence des services frontaliers du Canada (ASFC) et qui doivent être protégés sont répartis dans deux grandes catégories relatives aux préjudices que pourrait entraîner toute situation dans laquelle les ressources d'information seraient compromises pour les intérêts suivants :

1. Intérêt national

   On entend par « intérêt national » les renseignements et les biens concernant la sécurité du Canada ainsi que sa stabilité sociale, politique et économique.

2. Intérêt non national

   On entend par « intérêt non national » les renseignements et les biens concernant un intérêt autre que l'intérêt national, notamment les particuliers, les institutions gouvernementales et les entreprises, tels que les renseignements personnels, l'information sur l'application de la loi et les renseignements de nature concurrentielle tels que les secrets commerciaux, les renseignements de tiers, etc.

# Catégorisation

L'auteur ou le responsable de l'information doit appliquer un critère de préjudice pour établir le niveau de catégorisation du renseignement ou du bien. Si le renseignement ou le bien a été désigné comme étant de nature délicate et d'intérêt non national (protégé) ou d'intérêt national (classifié), le critère de préjudice ci-dessous doit être appliqué pour établir le degré de préjudice potentiel. Pour obtenir de l'aide, veuillez communiquer avec la Section de la sécurité de l'information, de la Direction de la sécurité et des normes professionnelles.

Pour ce faire, il faut procéder à une évaluation de la gravité du préjudice potentiel si la confidentialité, l'intégrité ou la disponibilité d'une ressource d'information était compromise. Si l'on détermine que le préjudice potentiel serait d'intérêt national, la catégorie appropriée serait sélectionnée parmi les catégories Confidentiel, Secret ou Très secret, selon l'ampleur du préjudice. Si l'on détermine que le préjudice potentiel serait d'intérêt non national, la catégorie appropriée serait alors sélectionnée parmi les catégories Protégé A, B ou C, selon l'ampleur du préjudice.







Lorsque le critère de préjudice est appliqué, les renseignements et les biens ne doivent en aucun cas être catégorisés de façon à :

- dissimuler des infractions à la loi, une pratique non efficiente ou une erreur administrative;
- éviter un embarras à un ministère, à une organisation ou à un fonctionnaire;
- limiter la concurrence;
- empêcher ou à retarder la publication de renseignements d'intérêt public qui ne nécessitent pas de protection.

La première étape consiste à déterminer, en fonction de l'une des deux principales catégories susmentionnées (intérêt non national ou intérêt national), si le renseignement ou le bien dont l'ASFC a la responsabilité est **protégé**, **classifié** ou **non classifié** au moment où il est créé ou recueilli.

**Renseignements et biens protégés**
Les renseignements et les biens sont considérés comme **protégés** si leur compromission pouvait causer un préjudice à un intérêt non national, comme un voyageur, un employé ou le mandat de l'ASFC. Voici des exemples de renseignements et de biens qui pourraient être considérés comme protégés :

- Renseignements personnels des employés (combinaison suffisante de renseignements personnels);
- Renseignements fournis par des tiers (renseignements opérationnels, financiers, commerciaux, scientifiques, techniques et de recherche fournis par des tiers ou les concernant);
- Procédure judiciaire et/ou application de la loi (renseignements relatifs à l'application de la *Loi sur les douanes* ou renseignements internes de l'ASFC);
- Recherches publiques
- Enquêtes (notamment les techniques et les plans);
- Discussions portant sur des ententes potentielles négociées (notamment l'échange de points de vue entre les employés);
- Comptes rendus de discussions sur des questions opérationnelles (comme le processus décisionnel interne et les opérations qui pourraient porter préjudice aux processus susmentionnés); et
- Renseignements portant sur la vulnérabilité de certains bâtiments ou ouvrages ou de réseaux ou systèmes divers, y compris des réseaux ou systèmes informatisés ou de communications, ou portant sur les méthodes employées pour leur protection.

Les renseignements biens protégés sont répartis en trois niveaux de catégorisation déterminés selon le degré de préjudice potentiel à l'intérêt non national, comme des particuliers, des entreprises ou des institutions gouvernementales.

| | |
|---|---|
| Catégorisation | Si la divulgation non autorisée pouvait, de manière raisonnable, causer un préjudice. |
| PROTÉGÉ C | Préjudice extrêmement grave à l'intérêt non national. Cette catégorie de renseignements, considérée comme étant de nature extrêmement délicate, s'applique à un nombre très restreint de renseignements dont le degré de préjudice potentiel est |







élevé. Par exemple : les renseignements concernant les informateurs dans une enquête criminelle ou d'autres renseignements concernant la sécurité de personnes ou l'exécution de la loi, dont la divulgation pourrait entraîner la mort de la personne.

PROTÉGÉ B — Préjudice grave à l'intérêt non national. Cette catégorie de renseignements, considérée de nature *particulièrement délicate*, existe en grande quantité et en forte concentration au sein de l'ASFC. La compromission de ces renseignements pose un risque de préjudice de niveau moyen à un citoyen ou à une organisation, comme le vol d'identité ou la perte d'un avantage concurrentiel. Ce niveau moyen de préjudice potentiel peut également être synonyme « de dommage ou d'embarras de longue durée » qui pourrait avoir des répercussions négatives directes sur la carrière, la réputation, la situation financière, la sécurité, la santé ou le bien-être d'une personne.

Les renseignements peuvent également être associés à la catégorie Protégé B du fait de leur nature, comme dans le cas d'enquêtes portant sur les infractions à la loi (dossiers des Enquêtes spéciales), le secret professionnel de l'avocat, et les documents de recherche scientifique présentés à l'ASFC.

PROTÉGÉ A — Préjudice à l'intérêt non national. Cette catégorie comprend les renseignements de nature *peu délicate* ou les renseignements personnels d'usage courant, par exemple, le salaire exact, qui s'ils étaient compromis pourraient causer un préjudice minimal ou entacher la réputation d'une personne ou d'une organisation.

**Renseignements biens classifiés**

Les renseignements et les biens sont considérés comme étant **classifiés**, si leur divulgation, leur modification, leur distribution ou leur destruction peut causer un préjudice à l'intérêt national, comme la défense et le maintien de la stabilité sociopolitique et économique du Canada. Des exemples de renseignements biens classifiés qui pourraient être considérés comme classifiés incluent, mais sans s'y limiter :

- Affaires fédérales-provinciales;
- Affaires internationales (comme des renseignements obtenus à titre confidentiel d'un gouvernement étranger);
- Défense du Canada (y compris les États alliés ou associés avec le Canada);
- Intérêts économiques du Canada, y compris des secrets industriels ou des renseignements financiers, commerciaux, scientifiques ou techniques appartenant au gouvernement du Canada ou à une institution fédérale et ayant une valeur importante ou pouvant vraisemblablement en avoir une;
- Application de la loi et enquêtes (comme des activités soupçonnées de constituer des menaces envers la sécurité du Canada au sens de la *Loi sur le Service canadien du renseignement de sécurité*); et
- Les documents confidentiels du Conseil privé de la Reine.







| | |
|---|---|
| Catégorisation | Si la divulgation non autorisée peut, de manière raisonnable, causer un préjudice. |
| TRÈS SECRET | Préjudice extrêmement grave à l'intérêt national. Renseignements concernant des hostilités armées potentielles contre le Canada ou ses alliés pour lesquels toute atteinte risquerait vraisemblablement de causer un préjudice exceptionnellement grave à l'intérêt national; par conséquent, ces renseignements seraient classifiés **Très secrets**. |
| SECRET | Préjudice grave à l'intérêt national. Des demandes de modifications législatives ou des détails sur des négociations internationales importantes justifient la catégorisation au niveau **Secret**. |
| CONFIDENTIEL | Préjudice à l'intérêt national. Les renseignements classifiés au niveau **Confidentiel**, comme les documents stratégiques sur les opérations de renseignement et sur le ciblage d'information ou des comptes rendus des discussions de comités fédéraux interministériels, pourraient vraisemblablement porter préjudice à l'intérêt national s'ils étaient compromis. |

**Renseignements ou biens non classifiés (non protégés ou classifiés)**
Si le renseignement ou le bien ne fait pas partie des catégories de renseignements ou de biens protégés ou classifiés, il n'est pas considéré comme étant de nature délicate et aucune mesure de sécurité particulière ne s'applique.

Remarque : Il est possible que les renseignements accessibles au public ne soient pas catégorisés comme étant protégés ou classifiés (toutefois, il se peut que dans certains cas, notamment les renseignements de source ouverte sur les activités du gouvernement, les renseignements ne soient pas classifiés comme étant du domaine public, mais une fois que le gouvernement les prend en compte, il les désigne comme étant de nature délicate et leur attribue une classification, p. ex. une menace interne pour les renseignements publics).

- Renseignements publiés ou offerts en vente à la population;
- Renseignements affichés sur le site Web de l'ASFC;
- Renseignements conservés dans les emplacements publics de l'ASFC;
- Renseignements déjà divulgués par l'autorité compétente au sein de l'ASFC conformément à la *Loi sur l'accès à l'information*.

La **désignation « Non classifié »** fait référence aux renseignements et aux biens dont la divulgation, la modification, la distribution ou la destruction ne causerait aucun préjudice à l'intérêt national ou à l'intérêt non national. Cette catégorisation ne signifie pas que ces renseignements ou ces biens peuvent être divulgués au public ni que le principe du besoin de connaître peut être éliminé. Les processus normaux d'accès à l'information s'appliquent toujours.





Le renseignement ou le bien qui ne comporte aucune marque de catégorisation n'a pas été évalué en fonction d'un critère de préjudice et il peut être considéré comme étant non classifié.

**Autres catégories spécialisées**

La mention « Document confidentiel du Conseil privé de la Reine » (document confidentiel du Cabinet) est une catégorie spécialisée dont la définition et le traitement est décrit dans la Politique sur la sécurité des documents confidentiels du Cabinet (2014) du Bureau du Conseil privé.



APPENDIX

| Renseignements DÉSIGNÉS | Intérêt AUTRE QUE NATIONAL |
|---|---|
| PROTÉGÉ A:<br>**Renseignements ou biens de nature peu délicate dont la compromission pourrait vraisemblablement porter un préjudice non lié à l'intérêt national (p. ex. plaintes ordinaires, renseignements généraux).** | Cote de fiabilité (CF)<br>**Il s'agit d'un niveau de sécurité et d'un prérequis pour une habilitation de niveau Secret ou Très Secret.** |
| PROTÉGÉ B<br>Renseignements ou biens de nature délicate dont la compromission pourrait vraisemblablement porter un préjudice sérieux non lié à l'intérêt national (p. ex. description d'une condition médicale, crime organisé). | |
| PROTÉGÉ C<br>Renseignements ou biens de nature très délicate dont la compromission pourrait vraisemblablement porter un préjudice extrêmement grave non lié à l'intérêt national (p. ex. renseignements sur une vie est en danger). | |
| **Renseignements CLASSIFIÉS** | |
| CONFIDENTIEL / SECRET:<br>Renseignements ou biens lorsque la compromission pourrait vraisemblablement porter un préjudice sérieux à l'intérêt national. | Habilitation de sécurité de niveau Secret |
| TRÈS SECRET:<br>Renseignements ou biens lorsque la compromission pourrait vraisemblablement porter un préjudice exceptionnellement grave à l'intérêt national. | Habilitation de sécurité de niveau Très Secret<br><br>Quelqu'un peut aussi avoir l'habilitation de sécurité de niveau Très Secret avec Endoctrinement, selon leurs fonctions. |





Canada Border Services Agency | Agence des services frontaliers du Canada



# Guidelines for the Classification and Handling of Information Assets

Information Security

Infrastructure and Information Security Division

Security and Professional Standards Directorate

27 January 2015



# Contents



These guidelines take effect on January 27, 2015.

This guideline contains some sample information supporting the classification and handling of information assets. This is basically a summary table which can quickly assist in the classification and handling of information / assets.

## 1. Protected Information Assets

**Protected** – the unauthorized disclosure of which could reasonably be expected to cause injury to a non-national interest.

| | Protected A | Protected B | Protected C |
|---|---|---|---|
| **Description** | Minor Injury if compromised.<br><br>Unauthorized disclosure could cause injury to an individual, organization or government, of Non-National interest<br><br>Loss of Privacy<br>Embarrassment | Medium to Serious Injury if compromised.<br><br>Unauthorized disclosure could cause serious injury to an individual, organization or government, of Non-National interest<br><br>Prejudicial treatment<br>Loss of reputation or competitive edge | Serious Injury if compromised.<br><br>Unauthorized disclosure could cause extreme grave injury to an individual, organization or government, of Non-National interest<br><br>Significant financial loss<br>Loss of life<br>Witness Protection Program<br>Informant Information |
| **Examples** | Inconvenience, damage to Departmental relationships, Degradation of public confidence.<br><br>Unsolicited proposals<br>Commercial and personal information<br>Home/business addresses and telephone numbers | Substantial duress to individuals, loss of competitive advantage, inability to conduct criminal investigations.<br><br>Personal information/biographical data<br>Medical/psychiatric/bank records<br>Competitive position of a third party<br>Trade secrets of a third party<br>Criminal information | Serious physical injury or loss of life, financial loss affecting viability of individual or business, undue hardship.<br><br>Information that could cause the bankruptcy of an individual or business.<br>Testimony against another individual |



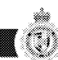




| | | | |
|---|---|---|---|
| | Date of birth/sex<br>Salaries<br>Contracts/standing offers<br>Combination of some information may result in classifying it at Protected B when you can totally identify a business or person | Performance evaluations<br>Religious or political beliefs<br>Information received "in confidence" from other government organizations<br>API/PNR information<br>Social insurance number plus another personal identifier | Witness Protection Program<br>Informant Information that could result in physical harm or death to an individual |
| **Physical Storage** | Container (e.g. file cabinet) with keyed lock in an operations zone<br>Operations Zone is defined as an area where access is limited to personnel who work there and to properly escorted visitors – example – Typical Government open office space | Approved security container (file cabinet or safe) with approved combination lock in an operations zone.<br>Operations Zone is defined as an area where access is limited to personnel who work there and to properly escorted visitors – example – Typical Government open office space | Approved security container (file cabinet or safe) with approved combination lock in a security zone.<br>Security Zone is defined as area to which access is limited to **authorized personnel and to authorized and properly escorted visitors.** Consult Security and Professional Standards Directorate for further information |
| **Electronic Storage** | Common or shared network drive<br>Portable media – Laptop (programmed with Agency approved encryption)<br>Blackberry with controlled access (User ID) not enabled with PIN to PIN communications<br>Diskettes, USB sticks, compact | Common or shared network drive<br>Portable media – Laptop (programmed with Agency approved encryption)<br>Blackberry – Encrypted with controlled access (User ID) not enabled with PIN to PIN communications<br>Diskettes, USB sticks, compact disks – labelled)<br>When using portable media, information | No Network storage<br>No hard drive Storage (C:\)<br>Stand-alone PC with removable hard drive and portable media – Laptop (programmed with Agency approved full disk encryption<br>Diskettes, USB sticks, compact disks – labelled |







| | | | |
|---|---|---|---|
| | disks – labelled.<br>When using portable media, information stored on these items must be transferred to Corporate Network drives and removed from portable media | stored on these items must be transferred to corporate network drives and removed from portable media.<br>Portable items (i.e. Agency Laptop) in an approved security container – locked when not in use | and must be encrypted.<br>Portable items (i.e. Agency Laptop) in an approved security container – locked when not in use |
| **Transmittal – Mail** | Reusable Interoffice envelope or gum sealed envelope / no security marking on envelope<br>Deliver using agency mailroom | **For both Internal and External Mail:**<br>2 gum sealed envelopes<br>Mark on inner envelope: "Protected B" – "to be opened by addressee only" or employees within a specific section.<br>Deliver using agency mailroom | 2 gum sealed envelopes<br>Mark on inner envelope: "Protected C" – "to be opened by addressee only"<br>Include Transmittal Note (GC44)<br>Notify recipient before sending and keep a record of the document<br>Deliver using agency mailroom |
| | **If Agency mailroom cannot be used, the following delivery methods may be used:<br>For Protected B and above, proof of mailing and a record of transit and delivery must be provided by the carrier.** | | |
| | Deliver through regular mail using a single, gum sealed envelope | Deliver using Canada Post priority courier or registered mail<br>Deliver using a private Courier<br>Outside Of Canada delivery by Diplomatic Security Mail Service | Deliver using Canada Post priority courier or registered mail<br>Deliver using a private Courier<br>Outside Of Canada delivery by Diplomatic Security Mail Service |
| **Electronic Transmission (Email & Fax)** | Regular email using the Agency's internal email system within and outside the | Email – PKI encryption or other approved encryption method<br>Secure "Protected" Facsimile Network | COMSEC Telecommunications Equipment.<br>Must not be emailed unless |

| | | | |
|---|---|---|---|
| | Agency, including Missions. Regular fax transmission within and outside the Agency. Missions – Secure "Protected" Facsimile Network consists of Fax equipped with fax encryption device. | consists of Fax equipped with fax encryption device. | using this equipment |
| **Print** | Network Printer or local Printer | Network Printer with PIN or local Printer | No network Printing Dedicated Local Printer in restricted area |
| **Telephone Communication** | Regular land-line phone communication in Canada and abroad, including Missions. Wireless communication is prohibited. | Regular land-line phone communication in Canada/US. Wireless communication is prohibited. COMSEC Telecommunications Equipment outside Canada/US including Missions | COMSEC Telecommunications Equipment |
| **Paper Destruction** | Hand shred and recycle | Approved Paper Shredder Consult with Regional or Headquarters Security or the Security and Professional Standards Directorate | Approved Paper Shredder Consult with Regional or Headquarters Security or the Security and Professional Standards Directorate |
| **Disposal** | Delete and empty recycle bin Overwrite compact disk, diskette, USB stick PC /Laptops/ Blackberry sanitized by IT before disposal | To securely delete all data on hard drive, with an approved disk sanitization utility (contact the Information Security Section of the Security and Professional Standards Directorate) **Note:** Portable media | Delete securely with an approved disk sanitization utility. Contact the Security and Professional Standards Directorate for advice and guidance. |





| | | | |
|---|---|---|---|
| | | including hard disks may require physical destruction (contact the Information Security Section of the Security and Professional Standards Directorate). | **Note**: Portable media including hard disks will require physical destruction (contact Information Security Section of the Security and Professional Standards Directorate. Missions – turn media over to CBSA Systems Administrator for appropriate destruction. |
| **Personnel Security Screening Requirement** | **Reliability Status** | **Reliability Status** | **Reliability Status** |
| **Underlying all of the above noted guidelines is the "need to know principle" which basically states that access to sensitive information should only be granted (given) to those individuals who will need to know the information in order to perform their duties.** | | | |

# 2. Classified Information Assets

**Classified** – the unauthorized disclosure of which could reasonably expected to cause injury to the national interest.

| | Confidential | Secret | Top Secret |
|---|---|---|---|
| **Description** | Unauthorized disclosure could cause an injury to the national interest | Unauthorized disclosure could cause serious injury to the national interest | Unauthorized disclosure could cause extremely grave injury to the national interest |
| **Examples** | Damage to relations, limited loss of public confidence.<br><br>Information related to negotiations with provinces<br>Strategies, tactics, political and economic report on other nations, not publicly available in Canada | Political tension, damage to critical infrastructure, civil disorder.<br><br>Minutes or Records of Cabinet Committees<br>Draft legislation<br>Strategies, tactics relating to international negotiations<br>Case files with national security implications | Widespread loss of life, Loss of continuity of government, irreparable loss of public confidence.<br><br>Important and significant negotiations<br>Vital law enforcement and Intelligence matters<br>Information classified by CSIS & RCMP regarding strategic plans, criminal or security threats |
| **Physical Storage** | Approved security container (file cabinet or safe) with approved combination lock in an Operations Zone "Operations Zone" is defined as an area to which access is limited to **authorized** personnel who work at the location and to **authorized** and properly escorted visitors. Consult with Regional Security or with Physical | Approved security container (file cabinet or safe) with approved combination lock in a Security Zone "Security Zone" is defined as an area where access is limited to **authorized** personnel who work at the location and to **authorized** and properly escorted | Approved security container (safe) with approved combination lock in a Security Zone. Note: when determined by a TRA and operational requirements, Top Secret material may be segregated and controlled within a closed community within a High Security Zone.<br>"High Security |

| | Confidential | Secret | Top Secret |
|---|---|---|---|
| | Security Section of the Security and Professional Standards Directorate for further information | visitors. | Zone" is defined as an area where access is limited to **authorized and appropriately screened** personnel who work at the location and to **authorized** and properly escorted visitors. |
| **Electronic Storage** | Contact the Security and Professional Standards Directorate. Requires Type I Crypto Missions, Consult with Security Officer | Contact the Security and Professional Standards Directorate. Requires Type I Crypto Missions, Consult with Security Officer | Specialized Secure Top Secret network (Contact Security and Professional Standards Directorate) No Blackberry For Missions, consult with Security Officer Portable media in a dial safe, in a high security zone. Locked when not in use. |
| **Transmittal – Mail** | 2 gum sealed envelopes Mark on inner envelope: "Confidential" – "to be opened by addressee only" Unmarked outer gum-sealed envelope Include Transmittal Note (GC44) Notify recipient before sending and keep a record of the document Deliver using agency mailroom | 2 gum sealed envelopes Mark on inner envelope: "Secret" – "to be opened by addressee only" Unmarked outer gum-sealed envelope Include Transmittal Note (GC44) Notify recipient before sending and keep a record of the document Deliver using agency mailroom | 2 gum sealed envelopes Mark on inner envelope: "Top Secret" – "to be opened by addressee only" Unmarked outer gum-sealed envelope Include Transmittal Note (GC44) Notify recipient before sending and keep a record of the document Deliver using agency mailroom |
| | **If Agency mailroom cannot be used, the following delivery** | | |







| | Confidential | Secret | Top Secret |
|---|---|---|---|
| | **methods may be used: For Protected B and above, proof of mailing and a record of transit and delivery must be provided by the carrier.** | | |
| | Deliver using Canada Post priority courier or registered mail<br>Deliver using a private Courier<br>Outside Of Canada delivery by Diplomatic Security Mail Service | Deliver using Canada Post priority courier or registered mail<br>Deliver using a private Courier<br>Outside Of Canada delivery by Diplomatic Security Mail Service | Deliver using Canada Post priority courier or registered mail<br>Deliver using a private Courier<br>Outside Of Canada delivery by Diplomatic Security Mail Service |
| **Electronic Transmission (Email & Fax)** | Must not be emailed.<br>Secure fax (connected to a COMSEC Telecommunication Equipment)<br>To the Missions – Consult with Security Officer | Must not be emailed.<br>Secure fax (connected to a COMSEC Telecommunicatio n Equipment)<br>To the Missions – Consult with Security Officer | Must not be emailed.<br>Secure fax (connected to a COMSEC Telecommunicatio n Equipment) |
| **Print** | No network Printing<br>Dedicated Local Printer in restricted area | No network Printing<br>Dedicated Local Printer in restricted area | No network Printing<br>Dedicated Local Printer in restricted area |
| **Telephone Communication** | connected to a COMSEC Telecommunication Equipment | connected to a COMSEC Telecommunicatio n Equipment | connected to a COMSEC Telecommunicatio n Equipment |
| **Paper Destruction** | Approved Paper Shredder must perform a crosscut operation with at least two, cross-oriented blade sets.<br>Consult with Regional Security or Security and Professional Standards | Approved Paper Shredder must perform a crosscut operation with at least two, cross-oriented blade sets.<br>Consult with Regional or Headquarters Security or the Security and Professional | Approved Paper Shredder must perform a crosscut operation with at least two, cross-oriented blade sets.<br>Consult with Regional or Headquarters Security or the Security and Professional |







| | Confidential | Secret | Top Secret |
|---|---|---|---|
| | Directorate | Standards Directorate | Standards Directorate |
| **Disposal** | Delete securely with an approved disk sanitization utility. **Note**: Portable media including hard disks will require physical destruction (contact Information Security Section of the Security and Professional Standards Directorate for advice and guidance). Missions – give media to Systems Administrator for destruction | Delete securely with an approved disk sanitization utility and contact Security and Professional Standards Directorate **Note**: Portable media including hard disks will require physical destruction (contact Information Security Section of the Security and Professional Standards Directorate for advice and guidance). Missions – give media to Systems Administrator for destruction | Delete securely with an approved disk sanitization utility and contact Security and Professional Standards Directorate **Note**: Portable media including hard disks will require physical destruction (contact Information Security Section of the Security and Professional Standards Directorate for advice and guidance). Missions – give media to Systems Administrator for destruction |
| **Personnel Security Screening Requirement** | **Confidential** | **Secret** | **Top Secret** |
| **Underlying all of the above noted guidelines is the "need to know principle" which basically states that access to sensitive information should only be granted (given) to those individuals who will need to know the information in order to perform their duties.** | | | |

When considering the purchase of a paper shredder, you should always assess what is the highest level of information being managed in your section or on your floor and select a shredder that will perform the adequate cutting for that highest level. Please consult with the local Regional or Headquarters Security Office or Security and Professional Standards Directorate for further assistance.

**Other Tips**:



Avoid sensitive discussions & exposing sensitive material where unauthorized people could overhear/see. Scrums, boom mikes, taxis, planes, public places, hotels.
Be aware that there is a risk of interception of hotel phone calls, and of long-distance calls outside Canada.
Ensure the person you disclose information to has the proper level of clearance to receive the information and has the "need to know this information" in order to perform their duties. Please practice and enforce the need to know principle.
Report to your Manager or the Regional or Headquarters Security Manager, as soon as possible, any actual or potential compromises of information or other assets.


Agence des services frontaliers du Canada | Canada Border Services Agency



# Lignes directrices en matière de classification et de traitement des ressources d'information

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

Le 27 janvier 2015

PROTECTION • SERVICE • INTÉGRITÉ

Canada



# Table des matières



Ces lignes directrices entre en vigueur le 27 janvier 2015.

Les présentes lignes directrices contiennent des renseignements facilitant la classification et le traitement des ressources d'information. Il s'agit fondamentalement d'un tableau sommaire qui permet de trouver rapidement les directives concernant la classification et le traitement des renseignements et des biens.

## 1. Renseignements et biens protégés

**Protégé** – Renseignements dont la divulgation sans autorisation risquerait vraisemblablement de causer un préjudice à des intérêts non nationaux.

| | **Protégé A** | **Protégé B** | **Protégé C** |
|---|---|---|---|
| **Description** | Préjudice léger si compromis<br><br>La divulgation non autorisée pourrait causer un préjudice à un intérêt non national, c'est-à-dire à une personne, à une organisation ou à un gouvernement<br><br>Atteinte au caractère confidentiel<br>Embarras | Préjudice moyen à grave si compromis<br><br>La divulgation non autorisée pourrait constituer un préjudice grave à un intérêt non national, c'est-à-dire à une personne, à une organisation ou à un gouvernement<br><br>Traitement préjudiciable<br>Atteinte à la réputation ou perte d'un avantage concurrentiel | Préjudice grave si compromis<br><br>La divulgation non autorisée pourrait causer un préjudice extrêmement grave à un intérêt non national, c'est-à-dire à une personne, à une organisation ou à un gouvernement<br><br>Perte financière importante<br>Décès<br>Programme de protection des témoins<br>Renseignements sur un informateur |
| **Exemples** | Inconvénients, torts aux relations ministérielles, diminution de la confiance du public<br><br>Propositions spontanées<br>Renseignements commerciaux et | Contrainte importante pour des personnes, perte d'un avantage concurrentiel, incapacité de mener des enquêtes criminelles<br><br>Renseignements personnels ou biographiques<br>Dossiers médicaux/psychiatrique | Blessure physique grave ou décès, perte financière touchant la viabilité d'une personne ou d'une entreprise, contrainte excessive<br><br>Renseignements |





| | | | |
|---|---|---|---|
| | personnels<br>Adresses et numéros de téléphone au domicile et au travail<br>Date de naissance et sexe<br>Salaires<br>Contrats/offres à commandes<br>La combinaison de certains renseignements peut donner lieu à la classification « Protégé B » lorsque l'on peut entièrement identifier une entreprise ou une personne | s/ bancaires<br>Compétitivité d'une tierce partie<br>Secrets commerciaux d'une tierce partie<br>Renseignements criminels<br>Évaluations du rendement<br>Croyances religieuses ou politiques<br>Renseignements obtenus « à titre confidentiel » d'autres organismes gouvernementaux<br>Renseignements préalables sur les voyageurs et dossiers passagers<br>Numéro d'assurance sociale et code d'utilisateur | pouvant entraîner la faillite d'une personne ou d'une entreprise.<br>Témoignage contre une autre personne.<br>Programme de protection des témoins<br>Renseignements sur les informateurs qui pourraient entraîner des préjudices physiques ou un décès |
| **Stockage physique** | Contenant (p. ex. classeur) avec une serrure à clé dans une zone de travail<br>L'expression « zone de travail » désigne une zone dont l'accès est réservé au personnel qui y travaille et aux visiteurs dûment accompagnés – p. ex. les bureaux à aire ouverte typiques du gouvernement | Contenant de sécurité approuvé (classeur ou coffre-fort) muni d'un cadenas à combinaison approuvé dans la zone de travail<br>L'expression « zone de travail » désigne une zone dont l'accès est réservé au personnel qui y travaille et aux visiteurs dûment accompagnés – p. ex. les bureaux à aire ouverte typiques du gouvernement | Contenant de sécurité approuvé (classeur ou coffre-fort) muni d'un cadenas à combinaison approuvé, dans une zone de sécurité<br>L'expression « zone de sécurité » désigne une zone dont l'accès est limité au **personnel autorisé et aux visiteurs autorisés et dûment accompagnés.**<br>Pour de plus amples renseignements, consultez la Direction de la sécurité et des normes professionnelles |

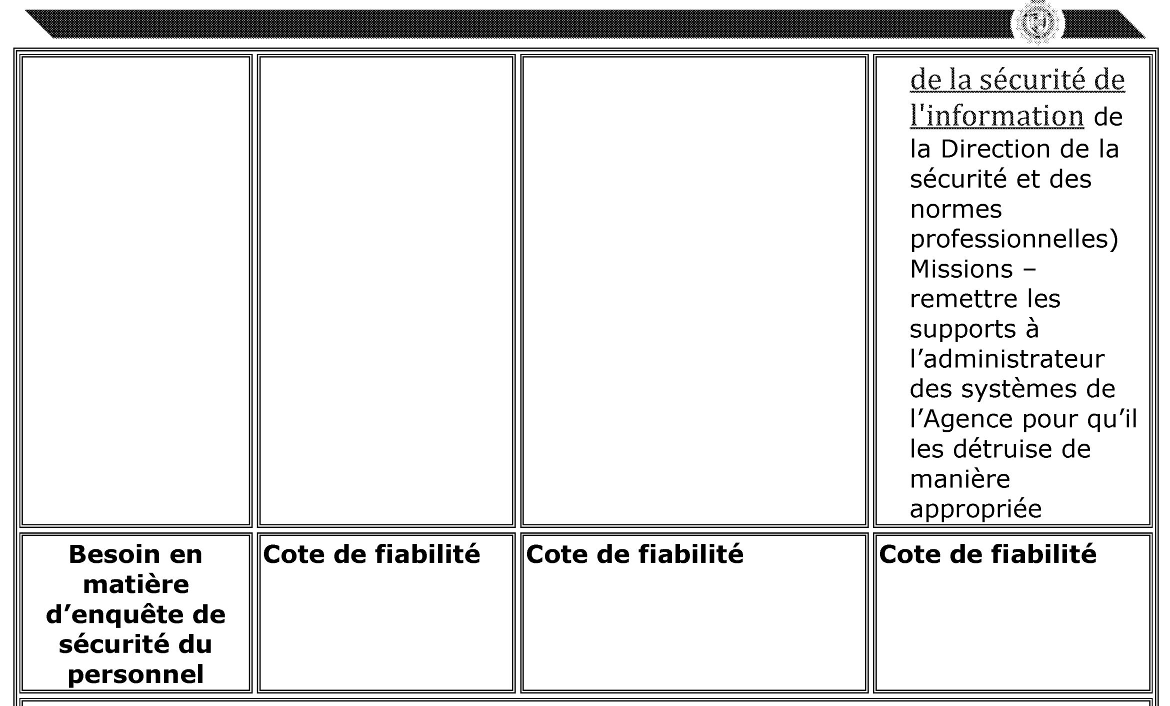
| | | | |
|---|---|---|---|
| **Stockage électronique** | Lecteur réseau commun ou partagé<br>Supports portatifs – Ordinateur portatif (programmé avec un logiciel de chiffrement approuvé par l'Agence)<br>Appareil BlackBerry avec accès contrôlé (identificateur d'utilisateur) qui n'est pas activé par des communications NIP à NIP<br>Disquettes, clés USB, disques compacts – étiquetés<br>Dans le cas d'un support portable, les renseignements qui y sont stockés doivent être transférés à un lecteur réseau de l'Agence et supprimés du support portable | Lecteur réseau commun ou partagé<br>Supports portatifs – Ordinateur portatif (programmé avec un logiciel de chiffrement approuvé par l'Agence)<br>Appareil BlackBerry – Chiffré avec accès contrôlé (identificateur d'utilisateur) qui n'est pas activé par des communications NIP à NIP<br>Disquettes, clés USB et disques compacts – étiquetés<br>Dans le cas d'un support portable, les renseignements qui y sont stockés doivent être transférés à un lecteur réseau de l'Agence et supprimés du support portable<br>Dispositifs portables (c.-à-d. ordinateur portatif de l'Agence) placés dans un contenant de sécurité approuvé (verrouillé lorsqu'il n'est pas utilisé) | Aucun stockage sur le réseau<br>Aucun entreposage sur le disque dur (C :\)<br>Ordinateur personnel autonome équipé d'un disque dur amovible et d'un support portable – Ordinateur portatif (programmé avec un logiciel de chiffrement du disque complet approuvé par l'Agence)<br>Disquettes, clés USB et disques compacts (étiquetés et chiffrés)<br>Dispositifs portables (c.-à-d. ordinateur portatif de l'Agence) placés dans un contenant de sécurité approuvé (verrouillé lorsqu'il n'est pas utilisé) |
| **Transmission (courrier)** | Enveloppe interne réutilisable ou enveloppe collée/aucun marquage de sécurité sur l'enveloppe<br>Envoyer en utilisant la salle du courrier de l'Agence | **Courrier interne et externe :**<br>Deux enveloppes collées<br>Marquer sur l'enveloppe intérieure : « Protégé B » – « Ne doit être ouvert que par le destinataire » ou certains employés au sein d'une section particulière<br>Envoyer en utilisant la salle du courrier de | Deux enveloppes collées<br>Marquer sur l'enveloppe intérieure : « Protégé C » – « Ne doit être ouvert que par le destinataire »<br>Inclure la note d'envoi (GC-44)<br>Avertir le destinataire avant l'envoi et conserver une |



| | | | |
|---|---|---|---|
| | | l'Agence | copie du document<br>Envoyer en utilisant la salle du courrier de l'Agence |
| | **Si la salle du courrier de l'Agence ne peut pas être utilisée, les méthodes de livraison suivantes peuvent être utilisées : pour les renseignements de niveau « Protégé B » et supérieur, la preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies par le transporteur.** | | |
| | Envoyer par courrier ordinaire dans une seule enveloppe collée | Envoyer en utilisant le courrier prioritaire de Postes Canada ou le courrier recommandé<br>Envoyer en utilisant un service de messagerie privé<br>À l'extérieur du Canada, envoi par le Service d'envois diplomatiques de sécurité | Envoyer en utilisant le courrier prioritaire de Postes Canada ou le courrier recommandé<br>Envoyer en utilisant un service de messagerie privé<br>À l'extérieur du Canada, envoi par le Service d'envois diplomatiques de sécurité |
| **Transmission électronique (courriel et télécopieur)** | Courriel ordinaire envoyé à l'aide du système interne de courriel de l'Agence à l'intérieur et à l'extérieur de l'Agence, y compris les missions<br>Transmission ordinaire de télécopies au sein et à l'extérieur de l'Agence<br>Missions – Réseau de télécopie « protégé » sécurisé comprenant un télécopieur doté d'un dispositif de chiffrement | Courriel – chiffrement de l'ICP ou autre méthode de chiffrement approuvée<br>Réseau de télécopie « Protégé » sécurisé comprenant un télécopieur doté d'un dispositif de chiffrement | Matériel de télécommunications COMSEC.<br>Ne doivent pas être envoyés par courriel, à moins d'utiliser ce matériel |



| | | | |
|---|---|---|---|
| **Impression** | Imprimante de réseau ou imprimante locale | Imprimante de réseau avec un NIP ou imprimante locale | Aucune impression sur le réseau Imprimante locale réservée à la zone d'accès limité |
| **Communication téléphonique** | Communication téléphonique ordinaire par ligne terrestre au Canada et à l'étranger, y compris les missions. La transmission au moyen de dispositifs de communication sans fil est interdite. | Communication téléphonique ordinaire par ligne terrestre au Canada et aux États-Unis. La transmission au moyen de dispositifs de communication sans fil est interdite. Matériel de télécommunication COMSEC à l'extérieur du Canada et des États-Unis, y compris les missions | Matériel de télécommunication COMSEC |
| **Destruction du papier** | Déchiquetage manuel et recyclage | Déchiqueteuse approuvée Consulter l'Unité de la sécurité de la région ou de l'Administration centrale ou la Direction de la sécurité et des normes professionnelles | Déchiqueteuse approuvée Consulter le Bureau de la sécurité régionale ou la Sécurité à l'Administration centrale ou la Direction de la |
| **Élimination** | Supprimer les fichiers, puis vider la corbeille Écraser le contenu du disque compact, de la disquette ou de la clé USB Les services de la TI doivent nettoyer les PC, les ordinateurs portatifs et les appareils BlackBerry avant de les éliminer | Supprimer de façon sécuritaire toutes les données des disques durs à l'aide d'un utilitaire de nettoyage de disque approuvé (communiquer avec la Division de la sécurité de l'information de la Direction de la sécurité et des normes professionnelles) **Remarque :** Les supports portables, y compris les disques durs, pourraient nécessiter une destruction physique (communiquer avec la Division de la sécurité de l'information de la Direction de la sécurité et des normes professionnelles) | Supprimer de façon sécuritaire toutes les données à l'aide d'un utilitaire de nettoyage de disque approuvé. Communiquer avec la Direction de la sécurité et des normes professionnelles pour obtenir des conseils et une orientation. **Remarque :** Les supports portables, y compris les disques durs, nécessiteront une destruction physique (communiquer avec la Division |



| | | | |
|---|---|---|---|
| | | | de la sécurité de l'information de la Direction de la sécurité et des normes professionnelles) Missions – remettre les supports à l'administrateur des systèmes de l'Agence pour qu'il les détruise de manière appropriée |
| **Besoin en matière d'enquête de sécurité du personnel** | **Cote de fiabilité** | **Cote de fiabilité** | **Cote de fiabilité** |
| **Toutes les lignes directrices susmentionnées sont fondées sur le principe du « besoin deconnaître » qui signifie essentiellement que l'accès aux renseignements de nature délicate doit être accordé seulement aux personnes qui en ont besoin pour s'acquitter de leurs tâches.** | | | |



## 2. Ressources d'information classifiées

**Classifié** – Renseignements dont la divulgation sans autorisation risquerait vraisemblablement de causer un préjudice à l'intérêt national.

| **Description** | **Confidentiel**<br>Une divulgation non autorisée pourrait causer un préjudice à l'intérêt national | **Secret**<br>Une divulgation non autorisée pourrait causer un préjudice grave à l'intérêt national | **Très secret**<br>Une divulgation non autorisée pourrait causer un préjudice extrêmement grave à l'intérêt national |
|---|---|---|---|
| **Exemples** | Détérioration des relations, perte limitée de la confiance du public<br><br>Renseignements liés aux négociations avec les provinces<br>Stratégies, tactiques, rapports politiques et économiques sur d'autres pays, qui ne sont pas accessibles au public au Canada | Tension politique, dommages causés à l'infrastructure essentielle, désordre civil<br><br>Procès-verbaux ou documents du Cabinet; Comités<br>Avant-projets de loi<br>Stratégies et tactiques concernant des négociations internationales<br>Dossiers ayant des répercussions sur la sécurité nationale | Nombreuses pertes de vie, perte de la continuité des opérations du gouvernement, perte irréparable de la confiance du public<br><br>Négociations importantes et significatives<br>Questions extrêmement importantes liées à l'exécution de la loi et au renseignement<br>Renseignements classifiés par le Service canadien du renseignement de sécurité et la Gendarmerie royale du Canada concernant des plans stratégiques, des activités criminelles ou des menaces pour la sécurité |
| **Stockage** | Contenant de sécurité | Contenant de | Contenant de |





| | Confidentiel | Secret | Très secret |
|---|---|---|---|
| **physique** | approuvé (classeur ou coffre-fort) muni d'un cadenas à combinaison approuvé dans une zone de travail<br>L'expression « zone de travail » désigne une zone dont l'accès est réservé au personnel **autorisé** qui y travaille et aux visiteurs **autorisés** et dûment accompagnés. Consulter l'Unité de la sécurité de la région ou la Section de la sécurité matérielle de la Direction de la sécurité et des normes professionnelles pour de plus amples renseignements | sécurité approuvé (classeur ou coffre-fort) muni d'un cadenas à combinaison approuvé dans une zone de sécurité<br>L'expression « zone de sécurité » désigne une zone dont l'accès est réservé au personnel **autorisé** qui y travaille et aux visiteurs **autorisés** et dûment accompagnés | sécurité approuvé (coffre-fort) muni d'un cadenas à combinaison approuvé dans une zone de sécurité<br>Remarque : Selon l'Évaluation des menaces et des risques et les exigences opérationnelles, certains renseignements Très secret seront séparés des autres et gardés par un groupe restreint dans une zone de haute sécurité<br>L'expression « zone de haute sécurité » désigne une zone dont l'accès est réservé au personnel **autorisé détenant la cote de sécurité appropriée** qui y travaille ainsi qu'aux visiteurs **autorisés** et dûment accompagnés |
| **Stockage électronique** | Communiquer avec la Direction de la sécurité et des normes professionnelles.<br>Une cryptographie de type I est requise.<br>Pour les missions, | Communiquer avec la Direction de la sécurité et des normes professionnelles<br>.<br>Une | Réseau spécialisé sécurisé « Très secret » (Communiquer avec la Direction de la sécurité et des |







| | Confidentiel | Secret | Très secret |
|---|---|---|---|
| | consulter l'agent de sécurité | cryptographie de type I est requise<br>Pour les missions, consulter l'agent de sécurité | normes professionnelles )<br>Aucun appareil BlackBerry.<br>Pour les missions, consulter l'agent de sécurité.<br>Supports portables dans un coffre-fort à combinaison, dans une zone de haute sécurité.<br>Verrouillé lorsqu'il n'est pas utilisé. |
| **Transmission (courrier)** | Deux enveloppes collées<br>Marquer sur l'enveloppe intérieure :<br>« Confidentiel » – « Ne doit être ouvert que par le destinataire »<br>Enveloppe collée externe sans aucune mention<br>Inclure la note d'envoi (GC-44)<br>Avertir le destinataire avant l'envoi et conserver une copie du document<br>Envoyer en utilisant la salle du courrier de l'Agence | Deux enveloppes collées<br>Marquer sur l'enveloppe intérieure :<br>« Secret » – « Ne doit être ouvert que par le destinataire »<br>Enveloppe collée externe sans aucune mention<br>Inclure la note d'envoi (GC-44)<br>Avertir le destinataire avant l'envoi et conserver une copie du document<br>Envoyer en utilisant la salle du courrier de l'Agence | Deux enveloppes collées<br>Marquer sur l'enveloppe intérieure :<br>« Très secret » – « Ne doit être ouvert que par le destinataire »<br>Enveloppe collée externe sans aucune mention<br>Inclure la note d'envoi (GC-44)<br>Avertir le destinataire avant l'envoi et conserver une copie du document<br>Envoyer en utilisant la salle du courrier de l'Agence |
| | **Si la salle de courrier de l'Agence ne peut pas être utilisée, les méthodes de livraison suivantes peuvent être utilisées : pour les renseignements de niveau « Protégé B » et supérieur, la preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies par le transporteur.** | | |

| | Confidentiel | Secret | Très secret |
|---|---|---|---|
| | Envoyer en utilisant le courrier prioritaire de Postes Canada ou le courrier recommandé<br>Envoyer en utilisant un service de messagerie privé<br>À l'extérieur du Canada, envoi par le Service d'envois diplomatiques de sécurité | Envoyer en utilisant le courrier prioritaire de Postes Canada ou le courrier recommandé<br>Envoyer en utilisant un service de messagerie privé<br>À l'extérieur du Canada, envoi par le Service d'envois diplomatiques de sécurité | Envoyer en utilisant le courrier prioritaire de Postes Canada ou le courrier recommandé<br>Envoyer en utilisant un service de messagerie privé<br>À l'extérieur du Canada, envoi par le Service d'envois diplomatiques de sécurité |
| **Transmission électronique (courriel et télécopieur)** | Ne doivent pas être envoyés par courriel<br>Télécopieur sécurisé (branché à du matériel de télécommunication COMSEC)<br>Aux missions – consulter l'agent de sécurité | Ne doivent pas être envoyés par courriel<br>Télécopieur sécurisé (branché à du matériel de télécommunication COMSEC)<br>Aux missions – consulter l'agent de sécurité | Ne doivent pas être envoyés par courriel<br>Télécopieur sécurisé (branché à du matériel de télécommunication COMSEC) |
| **Impression** | Aucune impression sur le réseau.<br>Imprimante locale réservée à la zone d'accès limité | Aucune impression sur le réseau.<br>Imprimante locale réservée à la zone d'accès limité | Aucune impression sur le réseau.<br>Imprimante locale réservée à la zone d'accès limité |
| **Communication téléphonique** | Combiné branché à du matériel de télécommunication COMSEC | Combiné branché à du matériel de télécommunication COMSEC | Combiné branché à du matériel de télécommunication COMSEC |
| **Destruction du papier** | Déchiqueteuse approuvée effectuant une coupe transversale et dotée d'au | Déchiqueteuse approuvée effectuant une | Déchiqueteuse approuvée effectuant une |





| | Confidentiel | Secret | Très secret |
|---|---|---|---|
| | moins deux ensembles de lames transversales Consulter l'Unité de la sécurité de la région ou la Direction de la Sécurité et des normes professionnelles | coupe transversale et dotée d'au moins deux ensembles de lames transversales Consulter l'Unité de la sécurité de la région ou de l'Administration centrale ou la Direction de la sécurité et des normes professionnelles | coupe transversale et dotée d'au moins deux ensembles de lames transversales Consulter l'Unité de la sécurité de la région ou de l'Administration centrale ou la Direction de la sécurité et des normes professionnelles |
| **Élimination** | Supprimer de façon sécuritaire toutes les données à l'aide d'un utilitaire de nettoyage de disque approuvé<br><br>**Remarque :** Les supports portables, y compris les disques durs, nécessiteront une destruction physique (communiquer avec la Division de la sécurité de l'information de la Direction de la sécurité et des normes professionnelles pour obtenir des conseils et une orientation) Missions – remettre les supports à l'administrateur des systèmes de l'Agence pour qu'il les détruise | Supprimer de façon sécuritaire toutes les données à l'aide d'un utilitaire de nettoyage de disque approuvé et communiquer avec la Direction de la sécurité et des normes professionnelles<br><br>**Remarque :** Les supports portables, y compris les disques durs, nécessiteront une destruction physique (communiquer avec la Division de la sécurité de l'information de la Direction de la sécurité et des normes professionnelles pour obtenir des conseils et une orientation) Missions – remettre les | Supprimer de façon sécuritaire toutes les données à l'aide d'un utilitaire de nettoyage de disque approuvé et communiquer avec la Direction de la sécurité et des normes professionnelles<br><br>**Remarque :** Les supports portables, y compris les disques durs, nécessiteront une destruction physique (communiquer avec la Division de la sécurité de l'information de la Direction de la sécurité et des normes professionnelles pour obtenir des conseils et une orientation) Missions – remettre les |



| | Confidentiel | Secret | Très secret |
|---|---|---|---|
| | | supports à l'administrateur des systèmes de l'Agence pour qu'il les détruise | supports à l'administrateur des systèmes de l'Agence pour qu'il les détruise |
| **Besoin en matière d'enquête de sécurité du personnel** | **Confidentiel** | **Secret** | **Très secret** |
| **Toutes les lignes directrices susmentionnées sont fondées sur le principe du « besoin de connaître » qui signifie essentiellement que l'accès aux renseignements de nature délicate doit être accordé seulement aux personnes qui en ont besoin pour s'acquitter de leurs tâches.** | | | |

Lorsque vous envisagez d'acheter une déchiqueteuse, vous devez toujours tenir compte du niveau le plus élevé de renseignements gérés au sein de votre section ou sur votre étage et sélectionner un appareil qui effectuera la coupe appropriée pour ce niveau. Veuillez consulter l'Unité de la sécurité de la région ou de l'Administration centrale ou la Direction de la sécurité et des normes professionnelles pour obtenir de l'aide supplémentaire.



**Autres conseils** :

Évitez de tenir des discussions sur des questions de nature délicate et de montrer du matériel de nature délicate lorsque des personnes non autorisées sont en mesure de les entendre ou de les voir (points de presse, micros-rails, taxis, avions, lieux publics, hôtels.

N'oubliez pas que les appels interurbains faits à l'étranger et les appels faits depuis les hôtels peuvent être interceptés.

Assurez-vous que la personne à qui vous communiquez les renseignements possède la cote de sécurité appropriée pour recevoir ces renseignements et qu'elle en a besoin pour s'acquitter de ses tâches. Veuillez appliquer le principe du « besoin de connaître ».

Signalez dès que possible à votre gestionnaire ou au gestionnaire de la sécurité de la région ou de l'Administration centrale toute compromission réelle ou potentielle des renseignements ou autres biens.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for Storage and Transport of Information Assets

Information Security

Infrastructure and Information Security Division

Security and Professional Standards Directorate

27 January 2015

PROTECTION • SERVICE • INTEGRITY





# Contents









# EFFECTIVE DATE

This standard is effective January 27, 2015.

# CONTEXT

Information is one of the most valuable assets to any organization and any loss of confidentiality, integrity, or availability of CBSA owned or accessed information/assets may result in harm to CBSA, its clients, and other stakeholders.

# APPLICATION

This standard is applicable to all CBSA management and employees (permanent, term, casual, part-time), contract and private agency personnel, and to individuals seconded or assigned to CBSA (including students); henceforth referred to as employees.

# STANDARD STATEMENT

## OBJECTIVE

The objective of this standard is to ensure that CBSA users adequately store and transport sensitive information assets, internal and external to the CBSA.

## EXPECTED RESULTS

The expected results of this standard are:

- Secure storage and transport of information assets according to their sensitivity level.
- Awareness of CBSA users of various means to adequately store and transport information / assets and of their responsibilities to safeguard them.







# REQUIREMENTS

## GENERAL

**Employees must:**

- Be fully aware of their security responsibilities regarding sensitive information / assets.
- Ensure that all information assets, throughout their life cycle, are secured against threats that have the potential to impact their confidentiality, integrity, availability, intended use and value.
- DO NOT, under ANY circumstances create, process, store or transmit classified information using any Agency Information Technology computer system connected to the Agency network unless a classified system has been designated specifically for use with classified information.
- If required contact the Security and Professional Standards Directorate (SPSD) for additional interpretation and guidance regarding the handling of information / assets.

## STORAGE WITHIN CBSA

**Employees must:**

- Physically control and securely store sensitive information / assets within controlled areas and in accordance with the RCMP G1-001, Security Equipment Guide ( http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm )
- Store assets of relatively high value (e.g. laptop computers) and portable storage devices, where feasible, in locked filing cabinets to reduce the risk of theft
- For Protected B information assets and above
    - Employ cryptographic mechanism to protect digital information in storage
    - Store non-digital information in in a locked filing cabinet (a container or a safe) specifically approved by the Security and Professional Standards Directorate (SPSD) for the level of sensitivity of the information or asset
    - In situations where it is not feasible to store sensitive information or assets in cabinets, the information may be kept in a secure room that is designed in accordance with specifications approved by the SPSD
    - Encrypt with Agency approved encryption algorithm(s), whether inside or outside Agency premises, including during transportation, ALL Protected B information stored on any portable media including but not limited to floppy disks, zip/jaz disks, CDs / DVDs, USB keys, server backup tapes, etc.







## TRANSPORT

### Employees must:

- Protect and control all sensitive information / assets (digital and non-digital) during transport outside of controlled areas using security measures, tailored to the sensitivity of the information / asset, in accordance with the TBS Operational Security Standard on Physical Security (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329&section=text ) and the RCMP Guide G1-009, Transport and Transmittal of Protected and Classified Information (http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009_e.pdf )
- Maintain accountability for information assets during transport outside of controlled areas
- Restrict the activities associated with transport of sensitive information assets to authorized personnel.
- For Protected B information assets and above:
  - Document activities associated with the transport of sensitive information assets.
  - DO NOT remove, store (either electronically or physically), process or use information assets off Agency premises unless approved by senior management in consultation with the Security and Professional Standards Directorate (SPSD).
  - Employ locked containers to protect the confidentiality and integrity of non-digital sensitive information during transport outside of controlled areas.
  - AVOID, whenever possible, the use of portable media (i.e. USB keys, portable hard drives, etc.) for storage of CBSA protected or classified information.
  - Ensure that portable storage devices are in an encrypted format using CBSA approved products and stored securely when used for sensitive CBSA information.
  - Ensure that agency-approved full disk encryption is installed on portable hard drives.
  - Physically protect any media in compliance with CBSA policies if media encryption is not technically feasible
- For Protected C, Confidential, Secret and Top Secret:
  - Ensure that an appropriate individual is identified as a custodian throughout the transport of information assets.
  - Ensure that the process is appropriately documented for audit trail purposes.

## *CONSIDERATIONS FOR EMAIL*

### Employees must:

- Limit the use of CBSA resources for personal emails to a reasonable amount.







- Refrain from sending chain letters or joke emails from a CBSA email account. These restrictions also apply to the forwarding of mail received by a CBSA employee/contractor/student, etc.
- Obtain approval from CBSA IT Security before sending information or warnings about viruses or other malware and mass mailings to CBSA employees.
- DO NOT use the CBSA email system for the creation or distribution of any disruptive or offensive messages, including offensive comments about (but not limited to) race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- Have reasonable limited expectation of privacy in anything that is stored, sent or received on the CBSA email system. CBSA reserves the right to monitor messages without prior notice, but is not obligated to monitor email messages.
- For Protected B
  - Ensure that digital information assets are encrypted using CBSA approved encryption before transmitting them using electronic mail.
- Protected C, Classified Secret and above information asset
  - DO NOT transmit by electronic mail under any circumstances.

### *CONSIDERATIONS FOR MAIL*

- Ensure, as a sender, that information assets are properly packaged before sending them to the mailroom or mailing them out directly.

### *CONSIDERATIONS FOR FAX*

- For Protected B information
  - Only transmit using an approved secure facsimile device.
- For Protected C and Classified information assets
  - DO NOT transmit by facsimile unless using a secure facsimile device approved by the Information Security Section of the SPSD.

### *CONSIDERATIONS FOR TELEPHONE*

- Apply caution in the type of information stored on telephone voicemail systems that are transported outside of controlled areas, as in most cases portable telephones do not have the identification, authentication and access control mechanisms typically employed in other information systems.
- Understand the sensitivity of information in all wireless communications and DO NOT discuss nor store Protected or Classified information on common cellular phones, PDAs, laptops, etc.
- Be aware that Information at the Protected A and Protected B levels can be communicated over ordinary telephone (land-lines), but not on wireless communications devices, and only to authorized individuals who have a legitimate "need-to-know", or to a client, and only if the information is concerning the client. Clients are to be advised of, and accept, the potential vulnerabilities, such as, eavesdropping or interception of calls by unauthorized individuals.



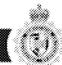




   - Ensure that for Protected C and above information assets, are only communicated using Agency approved secure telephone(s).

## CONSIDERATIONS FOR TELEWORK

- Employees are not to use their personal computing device or electronic devices when working at home (or outside of the CBSA) to store, process or access CBSA information. They must utilize CBSA/CRA corporate PCs, laptops or electronic devices (with approved logical access controls, encryption and a current anti-virus product) to store, process or access any CBSA information. The use of USB keys is prohibited.
- Encrypt sensitive information residing on portable electronic storage media using the approved CBSA encryption software.
- Mail sensitive information / assets from a Telework Place, using approved CBSA mailing procedures.
- It is the responsibility of management and the employee to ensure that the telework place where sensitive information / assets will be worked on or stored will meet all the criteria of this policy, and must consult the SPSD in case of doubt,
- Request that a manager (i.e. Assistant Director or Director) approve the removal of sensitive information / assets from CBSA premises and may consult the SPSD.
- Ensure that they secure sensitive information / assets in a locked briefcase or container approved by the SPSD when removing sensitive information from CBSA premises. The briefcase or container must be tagged with a forwarding or return address and/or phone number of the CBSA office.
- Ensure that paper files and other assets are only in vehicles during the conveyance between the employee's residence, place of work, and a client's place of business.
- Ensure that while travelling by vehicle, they are to secure sensitive information / assets in a locked briefcase or container and place it in a locked trunk or out of sight in a locked vehicle. Placement of the briefcase or container and/or the asset is to occur at the time of departure from the employee's residence, place of work or client's place of business.
- Make every reasonable effort to plan their itinerary to ensure that stopovers are eliminated before reaching a final destination. However, if brief unforeseen or planned stopovers are necessary (i.e. lunch, convenience store, daycare), employees should exercise good judgment and ensure that every reasonable effort has been made to minimize the risk to the sensitive information / assets.
- Ensure that Classified information and/or assets should never be left unattended in a vehicle.
- Ensure that while on public transit systems, employees maintain control of briefcases containing sensitive information / assets and are not to expose the material to the view of others.
- When travelling by aircraft, bus or train and when the material is too voluminous to be carried in locked briefcases, sensitive information / assets are to be stored in locked and approved containers tagged with forwarding or return address and checked-in as cargo luggage.



- Ensure that while between flights, buses or trains, employees are not to leave sensitive information / assets in traveller-convenience lockers usually found in bus terminals and train stations or other storage areas such as staffed storage facilities at airports.
- For Protected B information / assets
  - Ensure that outside the workplace, Protected B information is ~~only be~~ processed, stored or transmitted exclusively on CBSA computer systems that are protected by approved logical access controls and encryption.
  - Store, as much as possible, Information processed on the network and accessed by a CBSA approved remote capability, directly on the server (i.e. H: drive, G: drive, etc.).
  - Encrypt any information stored on the system's local hard drive using the CBSA approved full-disk encryption software.
  - Store classified and/or protected information and/or assets in locked and approved containers.
  - Store classified and/or protected waste in locked and approved containers until the material is destroyed.
  - When employees are occasionally allowed to work at home for short periods but are not in an authorized telework arrangement they may not have access to appropriate security containers. In such cases, store sensitive information / assets in locked and approved briefcases.

## *CONSIDERATIONS FOR COMMERCIAL ACCOMMODATIONS*

- Ensure that when in commercial accommodation; employees are to store sensitive information / assets in locked and approved briefcases or containers and place briefcases or containers out of sight.
- Employees are not to surrender sensitive information / assets to the commercial accommodation authorities for safekeeping.
- Ensure to place assets that are valuable and/or that can be used for criminal elements out of sight and, whenever practical, in a locked and approved container.

## *CONSIDERATIONS FOR CLIENT PREMISES*

- Store protected information and/or assets such as a laptop or notebook computer at a client's residence or place of business in an approved container, or in an approved filing cabinet provided by the client which can be secured by an approved CBSA combination padlock. The container or filing cabinet must also be secured in a locked room. It should be noted that a briefcase is not considered an approved container when left on client premises.
- Under no circumstances leave classified information and/or assets at a client's residence or place of business.







*** Note:** While it is impossible to address every situation in this standard, employees should as a general rule, exercise good judgment and ensure that every reasonable effort has been made to minimize the risk to sensitive information or assets, at all times. When in doubt, consult your immediate supervisor for guidance

## COMPLIANCE AND REPORTING

The CBSA Departmental Security Officer, security practitioners and managers are responsible for monitoring compliance with this standard within CBSA, measuring the effectiveness of identification, security categorization and marking of information resources and ensuring appropriate remedial actions are taken when deficiencies arise.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Manual, Reporting of Security Incidents.

## CONSEQUENCES

The DSO is responsible for investigating and responding to reports of non-compliance with this standard and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies, directives or standards may be subject to disciplinary action, up to and including termination of employment.

## STANDARD REVIEW

The DSO (Director General SPSD) should initiate a review of this standard at least every three years, or earlier, as required.

## REFERENCES


- TBS Operational Security Standard on Physical Security - https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329&section=text
- RCMP G1-001, Security Equipment Guide - http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm
- RCMP Guide G1-009, Transport and Transmittal of Protected and Classified Information - http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-eng.htm












# ENQUIRIES

Enquiries regarding this standard should be directed to:

**Security and Professional Standards Directorate**

E-mail: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Intranet : http://atlas/cb-dgc/sec/index_e.asp


Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme sur le stockage et le transport de ressources d'information

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

Le 27 janvier 2015

PROTECTION • SERVICE • INTÉGRITÉ




Agence des services frontaliers du Canada | Canada Border Services Agency



# Table des matières







# DATE D'ENTRÉE EN VIGUEUR

Cette norme entrera en vigueur le 27 janvier 2015.

# CONTEXTE

Les renseignements comptent parmi les biens les plus précieux de tout organisme, et toute atteinte à la confidentialité, à l'intégrité ou à la disponibilité des renseignements et des biens dont l'Agence des services frontaliers du Canada (ASFC) est propriétaire ou auxquels elle a accès peut causer préjudice à l'ASFC, à ses clients et à d'autres intervenants.

# APPLICATION

La présente norme s'applique à tous les gestionnaires et employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), aux contractuels et aux employés des agences privées ainsi qu'aux personnes en détachement ou affectées à l'ASFC (y compris les étudiants; ceux-ci seront ci-après désignés sous le nom d'employés.

# ÉNONCÉ DE LA NORME

## OBJECTIF

La présente norme vise à s'assurer que les utilisateurs de l'ASFC stockent et transportent de façon adéquate les ressources d'information internes et externes de nature délicate.

## RÉSULTATS ESCOMPTÉS

Les résultats escomptés de la présente norme sont comme suit :

- Le stockage et le transport sécuritaires des ressources d'information selon leur niveau de confidentialité.
- Les utilisateurs de l'ASFC connaissent les divers moyens de stocker et de transporter adéquatement les renseignements et les biens ainsi que leurs responsabilités à l'égard de la protection de ces derniers.



# EXIGENCES

## GÉNÉRALITÉS

**Les employés doivent s'assurer de ce qui suit :**

- Être pleinement informés de leurs responsabilités en matière de sécurité en ce qui concerne les renseignements et les biens de nature délicate.
- S'assurer que toutes les ressources d'information sont protégées tout au long de leur cycle de vie contre toute menace susceptible de porter atteinte à leur confidentialité, intégrité, disponibilité, utilisation prévue et valeur.
- S'ABSTENIR, en TOUTES circonstances, de créer, de traiter, de stocker ou de transmettre des renseignements classifiés au moyen du système informatique de technologie de l'information (TI) de l'Agence qui est connecté au réseau de cette dernière, à moins qu'un système classifié ait été désigné spécifiquement à cette fin.
- Communiquer au besoin avec la Direction de la sécurité et des normes professionnelles (DSNP) pour obtenir une interprétation et une orientation supplémentaires concernant le traitement des renseignements et des biens.

## STOCKAGE AU SEIN DE L'ASFC

**Les employés doivent s'assurer de ce qui suit :**

- Contrôler physiquement et stocker de façon sécuritaire les renseignements et les biens de nature délicate dans des zones contrôlées, conformément au Guide d'équipement de sécurité (G1-001) de la Gendarmerie royale du Canada (GRC) [http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm].
- Dans la mesure du possible, stocker les biens de valeur relativement élevée (p. ex. les ordinateurs portatifs) et les supports de stockage portatifs dans des classeurs verrouillés afin de réduire le risque de vol.
- Pour ce qui est des ressources d'information de niveau « Protégé B » ou supérieur :
    - Utiliser des mécanismes cryptographiques pour protéger les ressources d'information numériques stockées.







- Stocker les renseignements non numériques dans un classeur verrouillé (un contenant ou un coffre-fort) approuvé spécifiquement par la DSNP qui convient au niveau de confidentialité du renseignement ou du bien.
- Les renseignements ou les biens de nature délicate qui ne peuvent être stockés dans un classeur doivent être conservés dans une pièce sécuritaire conçue conformément aux spécifications approuvées par la DSNP.
- Chiffrer au moyen d'un algorithme de chiffrement approuvé par l'Agence TOUS les renseignements « Protégé B » stockés à l'intérieur ou à l'extérieur des locaux de l'Agence ou transportés sur un support portatif, tel qu'une disquette, un disque Zip ou Jaz, un CD ou un DVD, une clé USB, une bande de sauvegarde du serveur, etc.

## TRANSPORT

## Les employés doivent :

- Protéger et contrôler tous les renseignements et les biens (numériques ou non) de nature délicate durant leur transport hors des zones contrôlées en suivant des mesures de sécurité adaptées au niveau de confidentialité des renseignements ou des biens, conformément à la Norme opérationnelle sur la sécurité matérielle du Secrétariat du Conseil du Trésor (SCT) [http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329&section=text] et au document Transport et transmission de renseignements protégés ou classifiés (G1-009) de la GRC (http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-fra.htm).
- Demeurer responsables des ressources d'information durant leur transport hors des zones contrôlées.
- Limiter au personnel autorisé les activités liées au transport de ressources d'information de nature délicate.
- Pour ce qui est des ressources d'information de niveau « Protégé B » ou supérieur :
    - Consigner les activités liées au transport de ressources d'information de nature délicate.
    - S'ABSTENIR de retirer, de stocker (électroniquement ou physiquement), de traiter ou d'utiliser les ressources d'information à l'extérieur des locaux de l'Agence, à moins que ces opérations aient été approuvées par la haute direction en consultation avec la DSNP.
    - Utiliser des contenants verrouillés pour protéger la confidentialité et l'intégrité des ressources d'information non numériques de nature délicate durant leur transport hors des zones contrôlées.
    - ÉVITER, dans la mesure du possible, d'utiliser un support portatif (c.-à.-d. les clés USB, les disques durs portatifs) pour stocker les renseignements de l'ASFC protégés ou classifiés.







- S'assurer que les supports de stockage portatifs sont chiffrés au moyen de produits approuvés par l'ASFC et entreposés de façon sécuritaire lorsqu'ils sont utilisés pour stocker des renseignements de nature délicate de l'ASFC.
- S'assurer qu'un dispositif de chiffrement de disque complet approuvé par l'Agence est installé sur les lecteurs de disque dur portatifs.
- Protéger physiquement les supports de stockage conformément aux politiques de l'ASFC s'il n'est pas techniquement possible de les chiffrer.

- Pour ce qui est des ressources d'information de niveau « Protégé C », « Confidentiel », « Secret » et « Très secret » :
  - S'assurer que la bonne personne a été désignée comme gardien des ressources d'information tout au long de leur transport.
  - S'assurer que le processus est consigné de façon adéquate aux fins de piste d'audit.

### *POINTS À EXAMINER CONCERNANT LES COURRIELS*

## Les employés doivent :

- Limiter à un niveau raisonnable l'utilisation des ressources de l'ASFC à des fins personnelles.
- S'abstenir d'envoyer des chaînes de courriels ou des blagues à partir d'un compte de courriel de l'ASFC. Ces restrictions s'appliquent aussi à la transmission de courriels reçus par un employé de l'ASFC, un entrepreneur, un étudiant, etc.
- Obtenir l'approbation de la Division de la sécurité de la TI de l'ASFC avant d'envoyer aux employés de l'ASFC des renseignements ou des avertissements au sujet de virus ou d'autres logiciels malveillants et des envois massifs.
- S'abstenir d'utiliser les systèmes de courriel de l'ASFC pour la création ou la distribution de messages perturbateurs ou offensants, notamment des commentaires offensant sur la race, le sexe, la couleur, les incapacités, l'âge, l'orientation sexuelle, la pornographie, les croyances et les pratiques religieuses, les opinions politiques ou la nationalité.
- Avoir des attentes limitées et raisonnables en matière de protection de la vie privée en ce qui concerne tous les renseignements stockés ou reçus dans le système de courriel de l'ASFC ou envoyés par ce dernier. L'ASFC se réserve le droit de surveiller les messages sans préavis, mais elle n'est pas tenue de surveiller les courriels.
- Pour ce qui est des ressources d'information de niveau « Protégé B » :
  - S'assurer que les ressources d'information numériques sont chiffrées au moyen d'un dispositif de chiffrement approuvé par l'ASFC avant de les transmettre par courriel.
- Pour ce qui est des ressources d'information de niveau « Protégé C », « Secret » et de niveau supérieur :
  - S'ABSTENIR de les transmettre par courriel, quelles que soient les circonstances.







### POINT À EXAMINER CONCERNANT LA POSTE

- S'assurer, à titre d'expéditeur, que les ressources d'information sont correctement emballées avant de les transmettre à la salle de courrier ou de les poster directement.

### POINTS À EXAMINER CONCERNANT LE TÉLÉCOPIEUR

- Pour ce qui est des ressources d'information de niveau « Protégé B » :
  - Les transmettre uniquement au moyen d'un télécopieur sécurisé approuvé.
- Pour ce qui est des ressources d'information de niveau « Protégé C » et classifiées :
  - Éviter de les transmettre par télécopieur, à moins que ce soit au moyen d'un télécopieur sécurisé approuvé par la Division de la sécurité de l'information de la DSNP.

### POINTS À EXAMINER CONCERNANT LE TÉLÉPHONE

- Être vigilant quant aux types d'information stockés dans les systèmes de messagerie vocale téléphoniques qui sont transportés hors des zones contrôlées puisque dans la plupart des cas, les téléphones portatifs ne sont pas dotés de mécanismes d'identification, d'authentification et de contrôle d'accès normalement utilisés dans d'autres systèmes d'information.
- Comprendre la nature délicate des renseignements contenus dans tous les dispositifs de communication sans fil et S'ABSTENIR de stocker des renseignements protégés ou classifiés sur les téléphones cellulaires, les assistants numériques ou les ordinateurs portatifs communs ou d'en discuter sur ces appareils.
- Savoir qu'il est permis de communiquer des renseignements « Protégé A » et « Protégé B » par téléphone (ligne terrestre), mais non au moyen de dispositifs de communication sans fil et qu'il est possible de les communiquer seulement aux personnes autorisées qui ont un besoin de connaître légitime, ou à un client, et ce, seulement si les renseignements concernent ce dernier. Les clients doivent être avisés des vulnérabilités possibles, comme l'écoute clandestine ou l'interception des appels par des personnes non autorisées, et les accepter.

  - S'assurer que les ressources d'information de niveau « Protégé C » et supérieur ne sont communiquées qu'au moyen de téléphones sécurisés approuvés par l'Agence.

### POINTS À EXAMINER CONCERNANT LE TÉLÉTRAVAIL

- Les employés doivent s'abstenir d'utiliser leurs appareils informatiques ou électroniques personnels lorsqu'ils travaillent à la maison (ou à l'extérieur des locaux de l'ASFC) pour stocker ou traiter des renseignements de l'ASFC ou y accéder. Ils doivent utiliser les ordinateurs, les ordinateurs portatifs ou les appareils électroniques de l'ASFC ou de l'Agence du revenu du Canada (équipés de contrôles d'accès







logique, d'un logiciel de chiffrement et d'un antivirus à jour approuvés) pour stocker ou traiter tout renseignement de l'ASFC ou y accéder. L'utilisation de clés USB est interdite.

- Chiffrer les renseignements de nature délicate contenus dans les supports de stockage portatifs au moyen d'un logiciel de chiffrement approuvé par l'ASFC.
- Poster les renseignements et les biens de nature délicate à partir d'un lieu de télétravail en suivant les procédures relatives aux envois postaux approuvées par l'ASFC.
- Il appartient à la direction et à l'employé de s'assurer que le lieu de télétravail où des renseignements ou des biens de nature délicate seront traités ou entreposés satisfait à tous les critères de cette politique, et de consulter la DSNP en cas de doute.
- Demander qu'un gestionnaire (c.-à-d. un directeur adjoint ou un directeur) approuve le retrait de renseignements et de biens de nature délicate des locaux de l'ASFC et consulter la DSNP au besoin.
- S'assurer de sécuriser les renseignements et les biens de nature délicate dans une mallette verrouillée ou un contenant verrouillé approuvé par la DSNP lorsqu'ils les retirent des locaux de l'ASFC. La mallette ou le contenant doit être muni d'une étiquette indiquant l'adresse de renvoi ou de retour et/ou le numéro de téléphone du bureau de l'ASFC.
- Veiller à ce que les dossiers papier et les autres biens soient conservés dans le véhicule durant leur transport entre le domicile de l'employé, le lieu de travail et le lieu d'affaires du client.
- Lors de leur transport par véhicule, veiller à ce que les renseignements et les biens de nature délicate soient sécurisés dans une mallette verrouillée ou un contenant verrouillé placé dans un le coffre verrouillé du véhicule ou hors de vue dans le véhicule dûment verrouillé. Le dépôt de la mallette ou du contenant et/ou des biens dans le véhicule doit avoir lieu au moment du départ du domicile de l'employé, du lieu de travail ou du lieu d'affaires du client.
- Faire tous les efforts raisonnables pour planifier l'itinéraire afin de ne pas arrêter entre le lieu de départ et la destination finale. Toutefois, si de brefs arrêts, prévus ou non, sont nécessaires (c.-à-d. pour le dîner, faire une course au dépanneur ou passer à la garderie), les employés devraient faire preuve de jugement et veiller à déployer tous les efforts raisonnables pour réduire au minimum les risques qui menacent les renseignements et les biens de nature délicate.
- Veiller à ce que les renseignements et les biens classifiés ne soient jamais laissés sans surveillance dans un véhicule.
- Dans les transports publics, les employés doivent veiller à garder le contrôle des mallettes contenant les renseignements et les biens de nature délicate et éviter de les exposer à la vue des autres passagers.
- Lors des déplacements par avion, par autobus ou par train avec du matériel trop volumineux pour être transportés dans des mallettes verrouillées, les renseignements et les biens de nature délicate doivent être conservés dans des contenants verrouillés et approuvés munis d'étiquettes indiquant l'adresse de renvoi ou de retour; il faut enregistrer ces contenants comme des bagages.
- Entre les vols et les trajets en autocar ou en train, les employés ne doivent jamais laisser des renseignements et des biens de nature délicate dans les casiers que l'on trouve habituellement dans les







gares d'autocars et de trains ou dans d'autres aires d'entreposage, comme les installations d'entreposage avec personnel dans les aéroports.

- Pour ce qui est des renseignements et des biens de niveau « Protégé B » :
  - S'assurer qu'à l'extérieur du lieu de travail, les renseignements de niveau « Protégé B » ne sont traités, stockés et transmis qu'au moyen de systèmes informatiques de l'ASFC protégés par des contrôles d'accès logique et des dispositifs de chiffrement approuvés.
  - Dans la mesure du possible, stocker directement sur le serveur (c.-à-d. le lecteur H:, le lecteur G:) les renseignements traités sur le réseau et dont l'accès se fait au moyen d'une capacité à distance approuvée par l'ASFC.
  - Chiffrer au moyen d'un logiciel de chiffrement du disque complet approuvé par l'ASFC tout renseignement stocké sur le disque dur local du système.
  - Entreposer les renseignements et/ou les biens classifiés et/ou protégés dans des contenants verrouillés et approuvés.
  - Entreposer les rebuts classifiés et/ou protégés dans des contenants verrouillés et approuvés jusqu'à ce qu'ils soient détruits.
  - Il se peut que les employés autorisés à travailler à l'occasion à la maison pendant de courtes périodes ne participant pas à un régime de télétravail autorisé ne disposent pas de contenants de sécurité appropriés. Dans ces cas, les renseignements et les biens de nature délicate doivent être conservés dans des mallettes verrouillées et approuvées.

### *POINTS À EXAMINER CONCERNANT LES LOGEMENTS COMMERCIAUX*

- Lorsqu'ils se trouvent dans un logement commercial, les employés doivent s'assurer d'entreposer les renseignements et les biens de nature délicate dans des mallettes ou des contenants verrouillés et approuvés et de placer ces derniers hors de vue.
- Les employés ne doivent pas remettre des renseignements ou des biens de nature délicate aux autorités du logement commercial pour qu'ils les mettent en lieu sûr.
- S'assurer que les biens de valeur et/ou qui peuvent servir à des éléments criminels sont placés hors de vue et, si possible, dans un contenant verrouillé et approuvé.

### *POINTS À EXAMINER CONCERNANT LES LOCAUX DU CLIENT*

- Entreposer les renseignements et/ou les biens protégés, tels qu'un ordinateur portatif, au domicile ou au lieu d'affaires du client dans un contenant approuvé ou dans un classeur approuvé fourni par le client et qui peut être sécurisé au moyen d'un cadenas à combinaison approuvé par l'ASFC. Le contenant ou le classeur doit aussi être gardé dans une salle verrouillée. Il convient de noter qu'une mallette n'est pas considérée comme un contenant approuvé lorsqu'elle est laissée dans les locaux du client.
- Les employés ne devraient en aucun cas laisser des renseignements et/ou des biens classifiés au domicile ou au lieu d'affaires du client.







*** Nota :** Bien qu'il soit impossible de circonscrire toutes les situations possibles dans la présente norme, on demande généralement aux employés de faire preuve de jugement et de veiller en tout temps à déployer tous les efforts raisonnables pour réduire au minimum les risques qui menacent les renseignements ou les biens de nature délicate. En cas de doute, il faut consulter son superviseur immédiat pour obtenir des conseils.

## CONFORMITÉ ET RAPPORTS

L'agent de sécurité du ministère, les spécialistes de la sécurité et les gestionnaires de l'ASFC doivent surveiller la conformité à cette norme au sein de l'ASFC, mesurer l'efficacité de l'identification, de la catégorisation de sécurité et du marquage des ressources d'information, et veiller à ce que les mesures correctives appropriées soient prises lorsque des lacunes sont relevées.

Les employés signaleront les incidents de sécurité conformément aux exigences décrites dans le Volume de sécurité de l'ASFC, Signalement des incidents de sécurité.

## CONSÉQUENCES

L'agent de sécurité du ministère doit enquêter et intervenir lorsque des cas de non-conformité à la norme sont signalés, et voir à ce que les mesures correctives appropriées soient prises au moment opportun, s'il y a lieu. Toute violation des politiques, des directives ou des normes par un employé peut entraîner des mesures disciplinaires pouvant aller jusqu'au renvoi.

## EXAMEN DE LA NORME

L'agent de sécurité du ministère (directeur général, Direction de la sécurité et des normes professionnelles) devrait réaliser un examen de la norme tous les trois ans, ou à un intervalle plus court s'il le juge nécessaire.

## RÉFÉRENCES

- Norme opérationnelle sur la sécurité matérielle du SCT – https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329&section=text
- Guide d'équipement de sécurité (G1-001) de la GRC – http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm





- Transport et transmission de renseignements protégés ou classifiés (G1-009) de la GRC – http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-fra.htm

# DEMANDES DE RENSEIGNEMENTS

Pour toute demande de renseignements concernant la présente norme, veuillez communiquer avec :

**Direction de la sécurité et des normes professionnelles**

Courriel : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Intranet : http://atlas/cb-dgc/sec/index_f.asp

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for the Sanitization or Destruction of Information Assets

Information Security

Infrastructure and Information Security Division

Security and Professional Standards Directorate

December 1, 2015

PROTECTION • SERVICE • INTEGRITY





## Contents









# EFFECTIVE DATE

This standard is effective December 1, 2015.

# CONTEXT

## BACKGROUND

CBSA employees are responsible for the retention and disposal of their information and must therefore ensure that information is not inadvertently left on or is retrievable on media that is disposed of or is being re-deployed internally. The CBSA is responsible for the protection of information assets in its care, including personal information. Information inadvertently left on the electronic storage media could potentially cause unauthorized disclosure or use of sensitive information.

## AREAS OF CONCERN

The major issue regarding disposal of information storage assets is correctly managing the information stored on the asset prior to disposal.

There are two primary concerns:

1) Information may be left on the storage device after it leaves CBSA control, and is later retrieved and/or exploited by unauthorized personnel, and
2) Information which should be retained as an information record of business value (as per the Treasury Board Policy on Information Management, _, CBSA Records Retention and Disposition Guidelines and Procedures, CBSA Information Management (IM) Policy) is lost when the storage device is disposed of.

**Many factors amplify these concerns:**

- Where inventories of information are inaccurate or incomplete, it will be difficult to determine storage requirements, or what level of sensitivity the information has and may result in inappropriate storage or disposal.
- When information management procedures are manual or complex the information sensitivity maybe unknown, unclassified or classified incorrectly resulting in inappropriate storage or disposal.
- Small storage devices can retain vast quantities of information and can be easily lost and result in the exposure of significant Classified or Protected information/personal information
- Many organizations are involved in the lifecycle of information assets and where sound business practices and procedures for asset management are not in place, it can result in security or privacy breaches.







# APPLICATION

This standard is applicable to all CBSA management and employees (permanent, term, casual, part-time), contract and private agency personnel, and to individuals seconded or assigned to CBSA (including students).

# STANDARD STATEMENT

## OBJECTIVE

The objective of this standard is to ensure that CBSA users adequately sanitize or destroy information assets during disposal, release from CBSA control or release for re-use.

## EXPECTED RESULTS

The expected results of this standard are that:

- All information assets, digital and non-digital, whether or not considered removable, are properly sanitized or destroyed;
- All CBSA employees understand their roles and responsibilities as they relate to this standard; and
- Information is managed correctly and is not inadvertently disclosed.

# REQUIREMENTS

CBSA users must:

- Sanitize portable, removable storage devices prior to connecting such devices to the CBSA network (when authorized to connect such devices) (refer to ITSG-06 Clearing and Declassifying Electronic Data Storage, for details on sanitization according to Communications Security Establishment CSE);
- Physically protect and security store classified and protected information assets awaiting destruction (either on or off-site) using approved equipment, techniques and procedures;
- Destroy or sanitize, as applicable, information assets, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse;
- Clients who purchase/lease equipment which may be used to store/process CBSA information are responsible to ensure the proper disposal/destruction of this equipment at end of life;







- Employ sanitization and destruction mechanisms with strength and integrity commensurate with the classification or sensitivity of the information:
  - Ensure documentary evidence is generated and retained – either via certificate of destruction or confirmation report generated by cleansing mechanism –as verification/confirmation that data has been destroyed in a secure manner in accordance with CSEC policy ITSG-06 https://www.cse-cst.gc.ca/en/node/270/html/10572;
  - Ensure that the proper method of media destruction is used based upon the level of information stored on the media. Using the "delete" function to remove stored documents does not permanently remove the document from the media since a "deleted document" can be easily restored.
  - With respect to the disposal of classified and protected ***electronic*** assets, make use of the ITSG-06 guideline - Clearing and Declassifying Electronic Data Storage
  - The most efficient method of disposal for removable media, such as diskettes, CDs (CD-R, CD-RW), DVD-RW, USB drives, tapes, etc., is one of physical destruction. Diskette cartridges should be broken open and the "floppy diskette" inside cut into ½-inch strips. Tapes may also be cut into pieces. For the destruction of CD/DVD type media, it is recommended to use a device that will permanently "score" or grind off the surface of the disk.
- For transfers outside of the CBSA:
  - All storage media must be sanitized before equipment (either owned or leased – i.e. multi-function devices, photocopiers, etc.) is transferred outside of the CBSA or disposed of in any other means;
  - An inventory move must be created;
  - Drives must be removed and all electronic media (including removable devices) must be rendered unusable and physically shredded if possible prior to move outside of the Government of Canada;
  - Storage media devices under warranty that require replacement are to be managed in either of 2 ways: either the drive must be shredded/degaussed and replaced by the purchase of a new drive, or the defective drive must be sanitized (if possible), and returned to the vendor accompanied by a Certification of Destruction form. The form is completed by the vendor, and returned when the destruction of the drive (by mutually acceptable methods) has been verified.
  - If destruction of leased storage media is planned, then leasing arrangements must formally reference these standards and provision must be made for the compensation of the lessor for the removal and destruction of the storage media at the end of the lease. Defective storage media is to be handled using the same provisions as detailed above regarding warranty replacement.
- For transfers within the CBSA:







  - All storage media must be sanitized using appropriate and authorized media eraser;
  - An inventory move must be created
- Destroy information system media that cannot be sanitized;
- For Protected B and above information assets, apply the following measures:
  - Track, document and verify media sanitization and disposal actions; and
  - Test sanitization equipment and procedures to verify correct performance at least on a monthly basis
- For Protected C, Classified (Confidential, Secret and Top Secret) information assets, apply the following measures:
  - Follow Communications Security Establishment Canada (CSEC) policies and standards, and obtain guidance from the Infrastructure and Information Security Division, Security and Professional Standards Directorate as required.

# COMPLIANCE AND REPORTING

The CBSA Departmental Security Officer (DSO), security practitioners and managers are responsible for monitoring compliance with this standard within CBSA, measuring the effectiveness of identification, security categorization and marking of information resources and ensuring appropriate remedial actions are taken when deficiencies arise.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Manual, Reporting of Security Incidents.

# CONSEQUENCES

The DSO is responsible for investigating and responding to reports of non-compliance with this standard and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies, directives or standards may be subject to a review and possibly a revocation of their CBSA Reliability Status, disciplinary action, up to and including termination of employment.

# STANDARD REVIEW

The DSO (Director General, Security and Professional Standards Directorate) should initiate a review of this standard, at a minimum, every three years, or earlier as required.







# REFERENCES

- *RCMP G1-001 Security Equipment Guide*
- *CSEC ITSG-06 Clearing and Declassifying Electronic Data Storage Devices*
- *CSEC ITSD-03 Directive for the Control of COMSEC Material in the Government of Canada* -
- *Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment*

# ENQUIRIES

Enquiries regarding this standard should be directed to:

**Security and Professional Standards Directorate**

E-mail: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

# DEFINITIONS

Definitions related to this standard are included in the Security Terminology Glossary of the Security Manual.






Agence des services frontaliers du Canada
Canada Border Services Agency



# Norme pour le nettoyage ou la destruction des ressources d'information

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

Le 1er décembre 2015

PROTECTION • SERVICE • INTÉGRITÉ





# Table des matières









# Date d'entrée en vigueur

La norme est en vigueur depuis le 1er décembre 2015.

# CONTEXTE

## TOILE DE FOND

Les employés de l'Agence des services frontaliers du Canada (ASFC) sont responsables de la conservation et de l'élimination de leurs renseignements et doivent donc veiller à ce que ceux-ci ne soient pas laissés par inadvertance sur des supports en voie d'être éliminés ou redéployés à l'interne, ou ne puissent être extraits de tels supports. L'ASFC est responsable de la protection des ressources d'information en sa possession, y compris les renseignements personnels. Les renseignements de nature délicate laissés par inadvertance sur des supports électroniques sont susceptibles d'être divulgués ou utilisés de façon non autorisée.

## DOMAINES DE PRÉOCCUPATION

La principale difficulté liée à l'élimination des ressources de stockage d'information consiste à gérer correctement leur contenu avant leur élimination.

Les deux principales préoccupations sont les suivantes :

1) l'information peut être laissée sur un support une fois qu'elle n'est plus sous le contrôle de l'ASFC, puis être extraite et/ou exploitée par du personnel non autorisé;
2) l'information qui devrait être conservée en tant que ressource documentaire à valeur opérationnelle (conformément aux Politique sur la gestion de l'information (SCT), Conservation et Disposition des documents - Lignes Directrices et Procédures (ASFC), Politique de la gestion de l'information (GI) est perdue lorsque le support est éliminé.

**De nombreux facteurs amplifient ces préoccupations :**

- Lorsque les inventaires d'information sont inexacts ou incomplets, il est difficile de cerner les exigences en matière de stockage ou de déterminer le niveau de confidentialité de l'information et cela pourrait entraîner une élimination ou un stockage inapproprié.
- Quand les procédures de gestion de l'information sont manuelles ou complexes, le caractère délicat de l'information peut être inconnu, non classifié ou classifié incorrectement, entraînant ainsi une élimination ou un stockage inapproprié.
- Les petits supports de stockage peuvent contenir de vastes quantités d'information, être perdus facilement et entraîner l'exposition d'une grande quantité de renseignements classifiés ou protégés, dont des renseignements personnels.







- De nombreuses organisations jouent un rôle dans le cycle de vie des ressources d'information, et lorsqu'elles n'adoptent pas des pratiques et des procédures opérationnelles saines pour la gestion de ces ressources, elles ouvrent la porte à des violations potentielles de la sécurité ou d'atteintes à la vie privée.

# APPLICATION

La présente norme s'applique à tous les gestionnaires et employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), aux contractuels et aux employés des agences privées ainsi qu'aux personnes en détachement ou affectées à l'ASFC (y compris les étudiants).

# ÉNONCÉ DE LA NORME

## OBJECTIF

La présente norme a pour objectif de veiller à ce que les utilisateurs de l'ASFC nettoient ou détruisent adéquatement les ressources d'information pendant le processus d'élimination, de transfert hors du contrôle de l'ASFC ou de transfert en vue d'une réutilisation.

## RÉSULTATS ESCOMPTÉS

Les résultats escomptés de la présente norme sont comme suit :

- toutes les ressources d'information, numériques et non numériques, qu'elles soient considérées ou non comme amovibles, sont nettoyées ou détruites correctement;
- tous les employés de l'ASFC comprennent leurs rôles et responsabilités relativement à cette norme;
- l'information est gérée correctement et n'est pas divulguée par inadvertance.

# EXIGENCES

Les utilisateurs de l'ASFC doivent s'assurer de ce qui suit :

- nettoyer les supports amovibles et portables avant de les connecter au réseau de l'ASFC (lorsqu'une telle connexion est autorisée) [voir le Guide sur l'effacement et la déclassification des supports







d'information électroniques – ITSG-06, pour obtenir des détails sur le nettoyage conformément à la norme établie par le Centre de la sécurité des télécommunications;

- protéger physiquement et entreposer de manière sécuritaire les ressources d'information comportant des renseignements protégés et classifiés en attente de destruction, que ce soit sur place ou ailleurs, en utilisant de l'équipement, des techniques et des procédures approuvés;
- détruire ou nettoyer, s'il y a lieu, les ressources d'information, numériques et non numériques, avant leur élimination, leur transfert hors du contrôle de l'ASFC ou leur transfert en vue de leur réutilisation;
- les clients qui achètent ou louent de l'équipement pouvant être utilisé pour stocker et traiter l'information de l'ASFC doivent veiller à ce que cet équipement soit éliminé ou détruit correctement au terme de sa durée de vie utile;
- employer des mécanismes de nettoyage et de destruction dont la robustesse et l'intégrité correspondent à la classification ou au degré de confidentialité de l'information :
    - S'assurer que la preuve documentaire est produite et conservée – à l'aide d'un certificat de destruction ou d'un rapport de confirmation produit par un mécanisme de nettoyage – comme vérification ou confirmation que les données ont été détruites d'une manière sécuritaire conformément à la politique du CSTC Écrasement et déclassification des supports d'information électronique (ITSG-06) (https://www.cse-cst.gc.ca/fr/node/270/html/10572);
    - Voir à ce que la méthode appropriée de destruction de support soit utilisée en fonction du niveau de l'information stockée sur le support. L'utilisation de la fonction de suppression pour retirer les documents stockés ne permet pas de retirer les documents du support de façon permanente, car les documents supprimés peuvent être restaurés facilement.
    - En ce qui a trait à l'élimination des ressources ***électroniques*** classifiées et protégées, utiliser les lignes directrices – Guide sur l'effacement et la déclassification des supports d'information électroniques – ITSG-06.

    - La technique la plus efficace pour éliminer un média amovible, tel qu'une disquette, un CD (CD-R ou CD-RW), un DVD-RW, une clé USB ou une bande magnétique consiste en sa destruction physique. On doit briser la cassette d'une disquette, en ressortir celle-ci et la découper en bandes d'un demi pouce. On peut également découper en morceaux une bande magnétique. Pour détruire un média de type CD ou DVD, on recommande d'utiliser un dispositif capable de rayer ou meuler définitivement la surface.
- Pour les transferts à l'extérieur de l'ASFC :
    - les supports doivent être nettoyés avant que l'équipement (acheté ou loué – supports multifonctionnels, photocopieurs, etc.) ne soit transféré à l'extérieur de l'ASFC ou éliminé d'une tout autre façon;
    - un déplacement d'inventaire doit être créé;







  - les lecteurs doivent être retirés et les supports électroniques (dont les appareils amovibles) doivent être rendus inutilisables et détruits physiquement, si cela est possible, avant le transfert à l'extérieur du gouvernement du Canada;
  - les supports de stockage dont la garantie est valide et qui doivent être remplacés doivent être gérés de l'une de deux façons : soit le lecteur doit être détruit ou démagnétisé et remplacé par un nouveau lecteur, soit le lecteur défectueux doit être nettoyé (si cela est possible) et retourné au fournisseur accompagné d'un formulaire d'attestation de destruction. Le formulaire doit être rempli par le fournisseur puis retourné une fois la destruction du lecteur (au moyen de méthodes mutuellement acceptables) vérifiée.
  - Si l'on prévoit détruire des supports loués, les ententes de location doivent faire référence officiellement aux normes établies à cet égard et comporter une disposition relative au dédommagement du bailleur pour le retrait et la destruction des supports au terme du bail. Les supports défectueux doivent être traités conformément aux dispositions susmentionnées au sujet du remplacement lorsque la garantie est valide.
- Pour les transferts au sein de l'ASFC :
  - tous les supports doivent être nettoyés au moyen d'un dispositif d'effacement approprié et autorisé;
  - un déplacement d'inventaire doit être créé.
- Détruire les supports du système d'information qui ne peuvent pas être nettoyés;
- Pour les ressources d'information accompagnées d'une désignation de sécurité « Protégé B » ou supérieure, les mesures suivantes doivent être appliquées :
  - suivre, documenter et vérifier le nettoyage des supports et les activités d'élimination;
  - contrôler le matériel et les procédures de nettoyage au moins une fois par mois pour vérifier leur bon fonctionnement.
- Pour les ressources d'information « Protégé C », classifiées (Confidentiel, Secret, Très secret), les mesures suivantes doivent être appliquées :
  - Suivre les politiques et normes du Centre de la sécurité des télécommunications Canada (CSTC) et obtenir, au besoin, des directives de la part de la Division de l'infrastructure et de la sécurité de l'information, Direction de la sécurité et des normes professionnelles.







# CONFORMITÉ ET RAPPORTS

L'agent de sécurité du ministère, les spécialistes de la sécurité et les gestionnaires de l'ASFC doivent surveiller la conformité à cette norme au sein de l'ASFC, mesurer l'efficacité de l'identification, de la catégorisation de sécurité et du marquage des ressources d'information, et veiller à ce que les mesures correctives appropriées soient prises lorsque des lacunes sont relevées.

Les employés signaleront les incidents de sécurité conformément aux exigences décrites dans le Volume de sécurité de l'ASFC, Signalement des incidents de sécurité.

# CONSÉQUENCES

L'agent de sécurité du ministère (directeur général, Direction de la sécurité et des normes professionnelles) doit enquêter et intervenir lorsque des cas de non-conformité à la norme sont signalés, et voir à ce que les mesures correctives appropriées soient prises au moment opportun, s'il y a lieu. Toute violation des politiques, des directives ou des normes par un employé peut entraîner des mesures disciplinaires pouvant aller jusqu'au renvoi.

# EXAMEN DE LA NORME

L'agent de sécurité du ministère devrait réaliser un examen de la norme tous les trois ans, ou à un intervalle plus court s'il le juge nécessaire.

# RÉFÉRENCES

- *Guide d'équipement de sécurité (G1-001) de la Gendarmerie royale du Canada*
- Guide sur l'effacement et la déclassification des supports d'information électroniques – ITSG-06
- *ITSD-03 du CSTC – Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada*
- *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral*





# DEMANDES DE RENSEIGNEMENTS

Pour toute demande de renseignements concernant la présente norme, veuillez communiquer avec :

**Direction de la sécurité et des normes professionnelles**

Courriel : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

# DÉFINITIONS

Les définitions liées à la présente norme se trouvent dans le glossaire de terminologie sur la sécurité du Volume de la sécurité.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for the Transmittal of Sensitive Information/Assets

Information Security

Infrastructure and Information Security Division

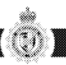
Security and Professional Standards Directorate

27 January 2015

PROTECTION • SERVICE • INTEGRITY

Canada

Canada Border Services Agency | Agence des services frontaliers du Canada



# Contents



# 1. Objective

The following standard is intended to securely transmit sensitive information securely, effectively and efficiently through a CBSA mailroom and if a CBSA mailroom should be used.

# 2. Exclusions

Procedures described in this standard do **NOT** apply to cash and negotiables, classified information such as Cabinet documents and federal budget related material. Such material must be transmitted in accordance with specific procedures approved by the Security and Professional Standards Directorate (SPSD). For information on these standards, contact the Regional Security Official or in Headquarters, the HQ Security Section.

# 3. Through a CBSA mailroom

## 3.1. Protected A Information

- For internal mailing a reusable (economy) envelope may be used.
- For mailing outside CBSA use a single gum-sealed envelope with no security marking.

## 3.2. Protected B Information, Protected C Information and Classified Information (Top Secret, Secret and Confidential)

- For Protected B Information, use two gum-sealed envelopes for mailing and for mailing both internally and externally to the CBSA. A security marking appears on the inner envelope *only*, while the address appears on both envelopes. The inner envelope should also be marked: "To be opened by addressee only" (e.g. in the case of employee performance appraisals or information that should be seen only by the addressee).
- For Protected C and Classified information (Top Secret, Secret and Confidential), use two gum-sealed envelopes. You **must** also enclose a self-addressed receipt (Form GC 44, Transmittal Note and Receipt) in the inner envelope, to be signed and returned by the recipient. You **must** keep a record of the Secret or Top Secret documents sent, and you **must** notify the intended recipient(s) before you ship the material.
- Send by priority courier, registered mail, private courier or diplomatic bag. Proof of mailing and a record of transit and delivery must be provided.



### 3.3. Sensitive Protected Information/Assets Bulky Shipments

- This material **must** be double-wrapped or put in a box sealed with tape and, if appropriate, covered with a wrapping. The outer wrapping must not have a security marking.
- Send by priority courier, registered mail, private courier or diplomatic bag. Proof of mailing and a record of transit and delivery must be provided by the carrier.

  * **Note** - An authorized employee with proper security clearance may also transport Sensitive information and assets between CBSA offices. The employee must ensure the information is enclosed within an envelope/wrapping within a security approved briefcase or other secure container (with a tag indicating a return office address or a telephone number, in case of loss), unless the information/assets are bulky. If the vehicle is used to transport the information/asset(s) the vehicle is not to be left unattended, and that the briefcase/package is locked in the trunk of the vehicle or, where this is not possible, at least out of sight in the locked vehicle. Sensitive information/assets are not to be left in a vehicle for storage.

## 4. If a CBSA mailroom cannot be used

### 4.1. Protected A Information

- Use a single gum-sealed envelope with no security marking when sent by mail. Reusable (economy) envelopes are not acceptable.

### 4.2. Protected B, Protect C or Classified Information (Top Secret, Secret, and Confidential)

- For Protected B Information, use two gum-sealed envelopes. A security marking appears on the inner envelope only, while the address appears on both envelopes. The inner envelope should also be marked: "To be opened by addressee only" (e.g. in the case of employee performance appraisals or information that should be seen only by the addressee).
- Send by priority courier, registered mail, private courier or diplomatic bag. Proof of mailing and a record of transit and delivery must be provided by the carrier.
- For Protected C or Classified information, you must enclose a self-addressed receipt (Form GC 44, Transmittal Note and Receipt) in the inner envelope, to be signed and returned by the recipient. You must keep a record of the Secret or Top Secret documents sent, and you must notify the intended recipient(s) before the shipment.
- Send by priority courier, registered mail, private courier or diplomatic bag. Proof of mailing and a record of transit and delivery must be provided.



## 4.3. Sensitive Information/Assets
### Bulky Shipments

- Double-wrap or put in a box sealed with tape and, if appropriate, covered with a wrapping. The outer wrapping must not have a security marking.
- Send by priority courier, registered mail, private courier or diplomatic bag. Proof of mailing and a record of transit and delivery must be provided by the carrier.
- For Protected C or Classified information, you must enclose a self-addressed receipt (Form GC 44, Transmittal Note and Receipt) in the inner envelope, to be signed and returned by the recipient. You must keep a record of the Secret or Top Secret documents sent, and you must notify the intended recipient(s) before the shipment.
- Send by priority courier, registered mail, private courier or diplomatic bag. Proof of mailing and a record of transit and delivery must be provided.

* **Note** - An authorized employee with proper security clearance may also transport Sensitive information and assets between CBSA offices. The employee must ensure the information is enclosed within an envelope/wrapping within a security approved briefcase or other secure container (with a tag indicating a return office address or a telephone number, in case of loss) unless the information and assets are bulky. If a vehicle is used to transport the information/asset, the vehicle is not to be left unattended, and that the briefcase/package is locked in the trunk of the vehicle, or where this is not possible, at least out of sight in the locked vehicle. Sensitive information/assets are not to be left in a vehicle for storage.

# 5. Transport and Transmittal

Maintaining authorized access to protected and classified assets and valuables is paramount when being transported.

- *When transporting protected and classified assets from one person or place to another, safeguards must include controlling access to the information by need-to-know.* This also applies to the servicing of containers.
- *When transmitting protected and classified assets from one person or place to another, safeguards must depend on proper packaging, an appropriate and reliable postal or courier service (government or private sector) and the anonymity of the information while in transit.*
- For the limited amount of protected and classified assets that are at higher risk, appropriate additional safeguards should be used, as indicated in the TRA.
- *Departments must transport or transmit protected and classified assets according to the minimum requirements set out in Appendix C.*
- Refer to RCMP Guide G1-009 - Transport and Transmittal of Sensitive Information and Assets for detailed specifications for enveloping, addressing and courier services for transporting and transmitting protected and classified assets.
- Departments are responsible for safeguarding security equipment (for example, security containers) during transport for servicing requirements.



## 6. Shipping and Receiving Areas, Loading Docks and Mail Rooms

Where possible, shipping and receiving areas, loading docks and mail rooms should not be directly linked or adjacent to restricted-access areas or critical facility infrastructure (such as water mains, cooling and heating systems, fire detection and alarm systems, electrical, telephone and data lines, and other service connections).



## Appendix A: Minimum Safeguards for the Transport and Transmittal of Protected and Classified Assets

| Activities | Protected A | Protected B | Protected C | Confidential | Secret | Top Secret |
|---|---|---|---|---|---|---|
| **Transport in Canada within restricted access area** | Transport Discretely | | *Single sealed envelope* with no security markings | Transport Discretely | | *Single sealed envelope* with no security markings |
| **Transport in Canada Outside restricted access area** | *Single sealed envelope* with no security markings appropriately addressed | | *Single sealed envelope* with security markings enclosed in a second secure enclosure (eg. locked brief case). | *Single sealed envelope* with no security markings appropriately addressed | | *Single sealed envelope* with security markings enclosed in a second secure enclosure (eg. locked brief case) |
| **Transport outside Canada within restricted access area** | Transport Discretely. Envelope not required | | *Single sealed envelope* with no security markings appropriately addressed | | | |
| **Transport outside Canada** | *Single sealed envelope* with no security markings appropriately addressed | | *Double sealed envelope.* | *Single sealed envelope* with no security markings | | *Double sealed envelope.* Security mark the inner envelope and appropriately address |





| | | | | |
|---|---|---|---|---|
| **Outside restricted access area** | | Security mark the inner envelope and appropriately address | appropriately addressed | |
| **Transmit in Canada within restricted access area** | Proprietary mail, messenger service or Departmental employee in a *single sealed envelope* with no security markings appropriately addressed | | | |
| **Transmit in Canada outside restricted access area** | Proprietary mail, messenger service, Departmental employee or communication letter mail (formerly first class mail) packaged in a *single sealed envelope* with no security markings appropriately addressed, or a *reliable courier service* or similar postal service with record of transit and delivery, packaged as for communication letter mail. Use this method only if delivery is urgent. | Proprietary mail, messenger service, or Departmental employee in a *double sealed envelope* with inner package security marked and appropriately addressed, or registered mail, in a *double sealed envelope* with inner | Proprietary mail, messenger service, Departmental employee or communication letter mail (formerly first class mail) packaged in a *single sealed envelope* with no security markings appropriately addressed, or a *reliable courier service* or similar postal service with record of transit and | Proprietary mail, messenger service, or Departmental employee in a *double sealed envelope* with inner package security marked and appropriately addressed, or registered mail, in a *double sealed envelope* with inner package security marked and appropriately addressed, or a *reliable courier service* or similar postal service *double sealed envelope* with inner package security marked and appropriately addressed with record of transit and delivery, packaged as for registered mail. Use this method only if delivery is urgent. |








| | | | | |
|---|---|---|---|---|
| | | package security marked and appropriately addressed, or a *reliable courier service* or similar postal service *double sealed envelope* with inner package security marked and appropriately addressed with record of transit and delivery, packaged as for registered mail. Use this method only if delivery is urgent. | delivery, packaged as for communication letter mail. Use this method only if delivery is urgent. | |
| **Transmit outside Canada within restricted access area** | In a *single sealed envelope* with no security markings appropriately | Proprietary mail, messenger service, or Departmental employee in a *single sealed envelope* with no security markings appropriately addressed | | |







| | | | | |
|---|---|---|---|---|
| | addressed. | | | |
| **Transmit outside Canada outside restricted access area** | *Single sealed envelope* with no security markings appropriately addressed and transmitted by, Proprietary mail, messenger service, or Departmental employee or communications letter mail, or a *reliable courier service* or similar postal service with record of transit and delivery, packaged as for registered mail. Use this method only if delivery is urgent. | *Appropriately screened* proprietary mail, messenger service *double sealed envelope* with a *Transmittal Form GC44* placed in the inner envelope. Security mark the inner envelope and seal with *approved tape,* or DFAIT mail service *double sealed envelope* with a Transmittal Form GC44 placed in the inner envelope. Security | *Appropriately screened* proprietary mail, messenger service packaged in a *single sealed envelope* with no security markings appropriately addressed, or a *reliable courier service* or similar postal service with record of transit and delivery, packaged in a *single sealed envelope* with no security markings appropriately addressed, or DFAIT mail service | *Appropriately screened* proprietary mail, messenger service *double sealed envelope* with a *SIARN* placed in the inner envelope. Security mark the inner envelope and seal with *approved tape*, or DFAIT mail service *double sealed envelope* with a *Transmittal Form GC44* placed in the inner envelope. Security mark the inner envelope and seal with *approved tape.* |







| | | | | |
|---|---|---|---|---|
| | | mark the inner envelope and seal with *approved tape.* | *double sealed envelope* with inner package security marked and appropriately addressed. | |

1. Single sealed envelope: A briefcase or other container of equal or greater strength, locked or sealed, can replace a single sealed envelope
2. Reliable Courier Service: The reliability of a courier service must be established through verification with other clients, or the Better Business Bureau, or the local police.
3. Approved Tape: Refer to PWGSC Security Equipment Catalogue or RCMP Guide G1-001 - Security Equipment Guide, to obtain information on the approved security tape.
4. Appropriately Screened Service: Personnel of the service are security screened to a level commensurate with the information or assets they control. See RCMP Guide G1-009 - Transport and Transmittal of Sensitive Information and Assets, for mailing procedures if personnel are not appropriately screened.
5. Double Sealed Envelope: When proprietary mail or messenger service is used, the outer envelope can be replaced by a briefcase or other container of equal or greater strength, locked or sealed. Additional measures may also apply such as when involving bulk shipment. See RCMP Guide G1-009 - Transport and Transmittal of Sensitive Information and Assets





Canada Border Services Agency | Agence des services frontaliers du Canada



# Normes sur la transmission de renseignements et de ressources de nature délicate

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

27 janvier 2015

PROTECTION • SERVICE • INTEGRITY

Canada



# Table des matières



# Objectif

La norme dont il est question dans ce document a pour objectif de permettre la transmission sécuritaire, efficace et efficiente de renseignements de nature délicate par l'entremise d'une salle du courrier de l'Agence des services frontaliers du Canada (ASFC), ainsi que d'établir si une salle du courrier de l'ASFC doit être utilisée.

# Exclusions

Les procédures décrites dans le cadre de cette norme **NE** s'appliquent **PAS** aux montants d'argent et autres éléments négociables, ainsi qu'aux renseignements classifiés, comme les documents du Cabinet et les documents relatifs au budget fédéral. Ces types de documents doivent être transmis en conformité avec les procédures précises approuvées par la Direction de la sécurité et des normes professionnelles (DSNP). Pour obtenir de plus amples renseignements sur ces normes, communiquez avec le responsable régional de la sécurité ou avec la Section de la sécurité à l'AC.

# Par l'entremise d'une salle du courrier de l'ASFC

## Renseignements Protégé A

- Pour le courrier interne, une enveloppe réutilisable (économie) peut être utilisée.
- Pour les envois postaux à l'extérieur de l'ASFC, utilisez une enveloppe scellée simple sans mention de sécurité.

## Renseignements Protégé B, renseignements Protégé C et information classifiée (Très secret, Secret et Confidentiel)

- Pour les renseignements Protégé B, utilisez deux enveloppes scellées, et ce, tant pour le courrier interne que pour le courrier externe. Une mention de sécurité figure sur l'enveloppe intérieure *seulement*, tandis que l'adresse est inscrite sur les deux enveloppes. L'enveloppe intérieure devrait aussi porter la mention « Ne doit être ouvert que par le destinataire » (p. ex. lorsqu'il s'agit d'évaluations du rendement de l'employé ou de renseignements auxquels seul le destinataire devrait avoir accès).
- Pour les renseignements Protégé C ou l'information classifiée (Très secret, Secret et Confidentiel), utilisez deux enveloppes scellées. Vous **devez** également inclure un reçu adressé (Formulaire GC-44, Note d'envoi et reçu) dans l'enveloppe intérieure, devant être signé et retourné par le destinataire. Vous **devez** noter au registre les documents « Secret » et « Très secret » envoyés, et informer le ou les destinataires prévus avant d'expédier les documents.
- Envoyez le tout en utilisant le courrier prioritaire, le courrier recommandé, un service de messagerie privé ou les valises diplomatiques. La preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies.



### Renseignements et ressources « Protégé » de nature délicate

#### Envois volumineux

- Ces documents **doivent** être envoyés dans un double emballage ou dans une boîte scellée au moyen de ruban adhésif et, au besoin, emballée. L'emballage extérieur ne doit porter aucune mention de sécurité.
- Envoyez le tout en utilisant le courrier prioritaire, le courrier recommandé, un service de messagerie privé ou les valises diplomatiques. La preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies par le transporteur.

  *** Remarque : Un employé autorisé possédant une autorisation de sécurité appropriée peut également transporter des renseignements et des ressources de nature délicate entre les bureaux de l'ASFC**. L'employé doit veiller à ce que l'information se trouve à l'intérieur d'une enveloppe ou d'un emballage, et à ce que cette enveloppe ou cet emballage soit transporté dans un porte-documents de sécurité approuvée ou un autre contenant sécurisé (portant une étiquette indiquant une adresse de bureau de retour ou un numéro de téléphone, en cas de perte), à moins que les renseignements et les ressources soient en grande quantité. Si les renseignements et les ressources sont transportés à bord d'un véhicule, celui-ci ne doit pas être laissé sans surveillance; l'employé doit veiller à ce que le porte-documents ou le colis soit placé dans le coffre arrière verrouillé du véhicule ou, sinon, hors de vue dans le véhicule dûment verrouillé. Les renseignements et les ressources de nature délicate ne doivent pas rester à l'intérieur d'un véhicule aux fins d'entreposage.

## Si une salle du courrier de l'ASFC ne peut être utilisée

### Renseignements Protégé A

- Lorsque les renseignements sont envoyés par courrier, utilisez une enveloppe scellée simple sans mention de sécurité. Les enveloppes réutilisables (économie) ne peuvent être utilisées.

### Renseignements Protégé B, renseignements Protégé C et information classifiée (Très secret, Secret et Confidentiel)

- Pour les renseignements Protégé B, utilisez deux enveloppes scellées. Une mention de sécurité figure sur l'enveloppe intérieure seulement, tandis que l'adresse est inscrite sur les deux enveloppes. L'enveloppe intérieure devrait aussi porter la mention « Ne doit être ouvert que par le destinataire » (p. ex. lorsqu'il s'agit d'évaluations du rendement de l'employé ou de renseignements auxquels seul le destinataire devrait avoir accès).
- Envoyez le tout en utilisant le courrier prioritaire, le courrier recommandé, un service de messagerie privé ou les valises diplomatiques. La preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies par le transporteur.



- Pour les renseignements Protégé C ou l'information classifiée, vous devez inclure un reçu adressé (Formulaire GC-44, Note d'envoi et reçu) dans l'enveloppe intérieure, devant être signé et retourné par le destinataire. Vous devez noter au registre les documents « Secret » et « Très secret » envoyés, et informer le ou les destinataires prévus avant d'expédier les documents.
- Envoyez le tout en utilisant le courrier prioritaire, le courrier recommandé, un service de messagerie privé ou les valises diplomatiques. La preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies.

### Renseignements et ressources de nature délicate

#### Envois volumineux

- Ces documents doivent être envoyés dans un double emballage ou dans une boîte scellée au moyen de ruban adhésif et, au besoin, emballée. L'emballage extérieur ne doit porter aucune mention de sécurité.
- Envoyez le tout en utilisant le courrier prioritaire, le courrier recommandé, un service de messagerie privé ou les valises diplomatiques. La preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies par le transporteur.
- Pour les renseignements Protégé C ou l'information classifiée, vous devez inclure un reçu adressé (Formulaire GC-44, Note d'envoi et reçu) dans l'enveloppe intérieure, devant être signé et retourné par le destinataire. Vous devez noter au registre les documents « Secret » et « Très secret » envoyés, prévenir le destinataire prévu avant l'envoi.
- Envoyez le tout en utilisant le courrier prioritaire, le courrier recommandé, un service de messagerie privé ou les valises diplomatiques. La preuve de l'envoi postal et une preuve de transmission et de réception doivent être fournies.

*** Remarque : Un employé autorisé possédant une autorisation de sécurité appropriée peut également transporter des renseignements et des ressources de nature délicate entre les bureaux de l'ASFC**. L'employé doit veiller à ce que l'information se trouve à l'intérieur d'une enveloppe ou d'un emballage, et à ce que cette enveloppe ou cet emballage soit transporté dans un porte-documents de sécurité approuvée ou un autre contenant sécurisé (portant une étiquette indiquant une adresse de bureau de retour ou un numéro de téléphone, en cas de perte), à moins que les renseignements et les ressources soient en grande quantité. Si les renseignements et les ressources sont transportés à bord d'un véhicule, celui-ci ne doit pas être laissé sans surveillance; l'employé doit veiller à ce que le porte-documents ou le colis soit placé dans le coffre arrière verrouillé du véhicule ou, sinon, hors de vue dans le véhicule dûment verrouillé. Les renseignements et les ressources de nature délicate ne doivent pas rester à l'intérieur d'un véhicule aux fins d'entreposage.



## Transport et transmission

Le maintien de l'accès autorisé aux biens de valeur et aux biens protégés et classifiés est primordial pendant leur transport.

- Pendant le transport de biens protégés et classifiés d'une personne ou d'un lieu à un autre, les mesures de protection à adopter doivent permettre de contrôler l'accès aux renseignements selon le principe du besoin de connaître. Cela s'applique également à l'entretien des contenants.
- Pendant la transmission de biens protégés et classifiés d'une personne ou d'un lieu à un autre, les mesures de protection à adopter doivent être axées sur l'emballage qui s'impose, ainsi que sur des services postaux et de messagerie fiables (gouvernement ou secteur privé) et sur le degré d'anonymat que ces renseignements peuvent conserver pendant le transport.
- Pour la quantité limitée de biens protégés et classifiés qui sont soumis à un risque plus élevé, il importe d'adopter des mesures additionnelles de protection, tel qu'il est indiqué dans l'Évaluation des menaces et des risques.
- Les ministères doivent transporter ou transmettre des biens protégés et classifiés conformément aux exigences minimales précisées à l'annexe C.
- Veuillez consulter le Guide de la Gendarmerie royale du Canada G1-009 - Transport ou transmission de renseignements protégés ou classifiés afin de connaître en détail les caractéristiques relatives aux enveloppes, aux adresses et aux services de messagerie à utiliser pour effectuer le transport et la transmission de biens protégés et classifiés.
- Les ministères sont responsables de la protection de l'équipement de sécurité, comme les contenants, pendant le transport nécessaire aux activités d'entretien.

## Zones d'expédition et de réception, quais de chargement et salles de courrier

Dans la mesure du possible, les zones d'expédition et de réception, les quais de chargement et les salles du courrier ne devraient pas être directement liés ou attenants à des zones d'accès restreint ou à l'infrastructure essentielle de l'immeuble (comme les canalisations principales, les systèmes de refroidissement et de chauffage, les systèmes de détection des incendies et les systèmes d'alarme, les circuits électriques, téléphoniques et de transmission de données, ainsi que les autres branchements).

# Annexe A : Mesures minimales de protection pour le transport et la transmission des biens protégés et classifiés

| Activités | Protégé A | Protégé B | Protégé C | Confidentiel | Secret | Très secret |
|---|---|---|---|---|---|---|
| **Transport au Canada à l'intérieur d'une zone à accès restreint** | Transporter avec discrétion. | | *Enveloppe simple scellée sans mention de sécurité.* | Transporter avec discrétion. | | *Enveloppe simple scellée sans mention de sécurité.* |
| **Transport au Canada à l'extérieur d'une zone à accès restreint** | *Enveloppe simple scellée sans mention de sécurité avec adresse appropriée.* | | *Enveloppe simple scellée avec mention de sécurité placée dans un second contenant sécuritaire (p. ex.* un porte-documents verrouillé). | *Enveloppe simple scellée sans mention de sécurité avec adresse appropriée.* | | *Enveloppe simple scellée avec mention de sécurité placée dans un second contenant sécuritaire (p. ex.* un porte-documents verrouillé). |
| **Transport à l'étranger à l'intérieur d'une zone à accès restreint** | Transporter avec discrétion. Enveloppe non requise. | | *Enveloppe simple scellée sans mention de sécurité avec adresse appropriée.* | | | |
| **Transport à** | *Enveloppe simple* | | *Enveloppe* | *Enveloppe simple* | | *Enveloppe double scellée. Mention de sécurité* |





| | | | | |
|---|---|---|---|---|
| **l'étranger à l'extérieur d'une zone à accès restreint** | *scellée sans mention de sécurité avec adresse appropriée.* | *double scellée. Mention de sécurité et adresse appropriée sur l'enveloppe intérieure.* | *scellée sans mention de sécurité avec adresse appropriée.* | *et adresse appropriée sur l'enveloppe intérieure.* |
| **Transmission au Canada à l'intérieur d'une zone à accès restreint** | Service postal ou de messagerie privé ou employé de l'Agence, dans une *enveloppe simple scellée* sans mention de sécurité avec adresse appropriée. | | | |
| **Transmission au Canada à l'extérieur d'une zone à accès restreint** | Service postal ou de messagerie privé, employé de l'Agence ou lettre de communication (ancien courrier de première classe) dans une *enveloppe simple scellée* sans mention de sécurité avec adresse appropriée, ou *service de messagerie fiable* ou service postal semblable avec preuve de transmission et de réception, emballé comme pour une lettre de communication. Méthode à utiliser | Service postal ou de messagerie privé, ou employé de l'Agence dans une *enveloppe double scellée* avec emballage intérieur portant la mention de sécurité et l'adresse appropriée, ou courrier recommandé, | Service postal ou de messagerie privé, employé de l'Agence ou lettre de communication (ancien courrier de première classe) dans une *enveloppe simple scellée* sans mention de sécurité avec adresse appropriée, ou *service de messagerie fiable* ou service postal semblable avec | Service postal ou de messagerie privé ou employé de l'Agence, dans une *enveloppe double scellée* avec emballage intérieur portant la mention de sécurité et l'adresse appropriée, ou courrier recommandé, dans une *enveloppe double scellée* avec emballage intérieur portant la mention de sécurité et l'adresse appropriée, ou *service de messagerie fiable* ou service postal semblable dans une *enveloppe double scellée* avec emballage intérieur portant la mention de sécurité et l'adresse appropriée avec preuve de transmission et de réception, emballé comme pour le courrier recommandé. Méthode à utiliser seulement si la livraison est urgente. |





| | | | | |
|---|---|---|---|---|
| | seulement si la livraison est urgente. | dans une *enveloppe double scellée* avec emballage intérieur portant la mention de sécurité et l'adresse appropriée, ou *service de messagerie fiable* ou service postal semblable dans une *enveloppe double scellée* avec emballage intérieur portant la mention de sécurité et l'adresse appropriée avec preuve de transmission et de réception, emballé comme pour le courrier | preuve de transmission et de réception, emballé comme pour une lettre de communication. Méthode à utiliser seulement si la livraison est urgente. | |





| | | | | |
|---|---|---|---|---|
| | | recommandé. Méthode à utiliser seulement si la livraison est urgente. | | |
| **Transmission à l'étranger à l'intérieur d'une zone à accès restreint** | *Enveloppe simple scellée* sans mention de sécurité avec adresse appropriée. | Service postal ou de messagerie privé ou employé de l'Agence, dans une *enveloppe simple scellée* sans mention de sécurité avec adresse appropriée. | | |
| **Transmission à l'étranger à l'extérieur d'une zone à accès restreint** | *Enveloppe simple scellée sans mention de sécurité avec adresse appropriée, et transmission par un service postal ou de messagerie privé, un employé de l'Agence ou une lettre de communication, ou un service de messagerie fiable ou un service postal semblable avec preuve de transmission et de réception, emballé comme pour le courrier recommandé.* Méthode à utiliser | *Service postal ou de messagerie privé répondant aux normes de sécurité du personnel dans une enveloppe double scellée dont l'enveloppe intérieure contient un formulaire de transmission GC-44*. Mention de | *Service postal ou de messagerie privé répondant aux normes de sécurité du personnel dans une enveloppe simple scellée sans mention de sécurité avec adresse appropriée, ou service de messagerie fiable ou* | *Service postal ou de messagerie privé répondant aux normes de sécurité du personnel dans une enveloppe double scellée dont l'enveloppe intérieure contient un Récépissé de renseignements et de biens délicats. Mention de sécurité sur l'enveloppe intérieure et sceau avec ruban approuvé, ou service de courrier du MAECD dans une enveloppe double scellée dont l'enveloppe intérieure contient un formulaire de transmission GC-44.* Mention de sécurité sur l'enveloppe intérieure et sceau avec *ruban approuvé*. |





| | | | | |
|---|---|---|---|---|
| | seulement si la livraison est urgente. | sécurité sur l'enveloppe intérieure et sceau avec *ruban approuvé*, ou service de courrier du MAECD dans une *enveloppe double scellée* dont l'enveloppe intérieure contient un formulaire de transmission GC44. Mention de sécurité sur l'enveloppe intérieure et sceau avec *ruban approuvé.* | *service postal semblable avec preuve de transmission et de réception, emballé dans une enveloppe simple scellée sans mention de sécurité avec adresse appropriée, ou service de courrier du MAECD dans une enveloppe double scellée dont l'emballage intérieur porte la mention de sécurité et l'adresse appropriée.* | |





# Appendix 1: Inventory Template

## Steps to follow

Label each USB key with a control number to keep track of the keys more efficiently.
The control number should include a non-identifiable coding for the **highest level** of information contained on the USB key, the name or acronym of the Directorate, of the Division and an assigned number.

The following is an **example** of non-identifiable coding and its corresponding information level:

**A** = Unclassified information;
**B** = Protected information;
**C** = Secret information;
**D** = Top Secret information;

Therefore, the control number for unclassified information contained on a USB key belonging to the Resource Management Directorate (RMD), Financial Planning Division (FINPLAN), would be ARMDFINPLAN##.

## Étapes à suivre

Inscrire sur chaque clé USB un numéro de contrôle pour assurer un suivi plus efficace des clés.
Le numéro de contrôle doit comprendre un codage non identifiable pour le **niveau** d'information l**e plus élevé** figurant dans la clé USB, le nom ou acronyme de la Direction, de la Division et un numéro attribué.

Voici un **exemple** de codage non identifiable et le niveau d'information correspondant :

**A** =information non classifiée;
**B** = information protégée;
**C** = information de niveau Secret;
**D** = information de niveau Très secret;

Ainsi, le numéro de contrôle de l'information non classifiée figurant dans une clé USB appartenant à la Direction de la gestion des ressources (DGR), de la Division de la planification financière (DPF), porterait le numéro ADGRDPF##.






# Procedures for the use of Portable Data Storage Devices within CBSA



PROTECTION • SERVICE • INTEGRITY





# Contents



These procedures take effect on December 22, 2015.

## 1. Objective

The following procedures are intended to highlight the responsibilities of authors and/or recipients to properly handle information or assets relating to the use of Portable Data Storage Devices (hereafter referred to as "portable device"). Protection of information assets is the primary goal of information security. This includes practicing safe computing behaviors to reduce the overall occurrence of theft, loss, or misuse of government information assets. A breach in information security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach.

**These procedures apply to all CBSA information and/or any type of information handled by CBSA employees/contractors transmitted or stored on portable devices.**

Another objective is to establish minimum standards for utilizing and protecting CBSA information data transmitted or stored on portable devices (i.e. USB keys, flash memory, CDs/DVDs, external hard drives etc.). Portable devices can be a convenient aspect of CBSA business; however, due to their size they are easily lost or stolen and may cause a security breach. Portable devices are increasing in storage capacity and can store large quantities of files and information. Portable Digital Assistants (PDAs), BlackBerrys, iPods and other media players have the ability to store files and can be included as portable devices.

The prevalence of these devices within CBSA has led to significant support issues and security risks. While the cost of replacing the devices is relatively insignificant, more and more users store sensitive information on these devices, and therefore results in a data leakage threat. Additionally, use of portable devices can introduce a number of security threats to the CBSA network, including malware, viruses, or worms.

## 2. Consequences of Breaches

**The consequences of breaches may include (but not limited to):**

- Disclosure of personal information and/or operational data;
- Propagation of potentially unwanted malware, viruses, spyware, and other unsavory types of software;
- Interruption in government's ability to deliver services;
- Financial losses related to correcting the situation;
- Threats to public safety or individuals' health and well-being;
- Legal actions; and
- Erosion of the public trust in the government.



**Areas of Concern**

The primary area of concern is the risk of portable devices being lost, stolen or improperly used and government information being inappropriately disclosed, altered or destroyed.

*Many factors amplify this concern:*

- Use of personal and unauthorized devices can result in privacy and security breaches (i.e. personal USB devices, music/video media players, etc.).
- The size of portable devices increases the likelihood of physical loss or theft.
- If processes are not in place to allow for prompt reporting of the loss, theft or damage of devices the potential for information being inappropriately disclosed, altered or destroyed is increased.
- Unsecured or poorly secured devices increase the security and privacy risks to information and information resources.
- Portable devices can have large storage capacity which can allow for the theft of large amounts of data or applications.
- Proliferation of malware/viruses on these devices from a variety of sources (such as giveaways at trade shows, devices being inspected at various border points, non-certified devices being charged on desktop laptops, etc.). The sources are very extensive and lengthy.
- Where portable devices are used there may be a lack of enterprise-level management tools for managing their use and disposal.
- Where portable devices are used to transport CBSA information, security measures such as encryption may not be implemented.

## 3. Use of Portable Data Storage Devices in CBSA

In order to limit risk to the Agency, CBSA employees (this includes: permanent, term, casual, part-time, contract and private agency personnel, and to individuals seconded or assigned to CBSA (including students) must **always**:

- Avoid the use of portable devices where technically possible, and to limit use when absolutely required.
- Limit the use of portable devices for the temporary storage of a copy of CBSA information only.
- Limit the use to those issued, and inventoried, by the CBSA.
- Ensure all portable devices are password or biometric controlled and the CBSA information stored on them is encrypted.
- Ensure portable devices are handled, stored, and transported in accordance with the classification level of data.
- Return all portable storage devices to the inventory; once the temporary requirement has been met (refer to Section 4).
- Immediately report any loss or theft of a portable storage device (refer to Section 9).



CBSA employees must **never**:

- Use a "personal" portable device to store CBSA Information, or connect a personal device to the CBSA Network (use of "personal" portable devices is prohibited).
    - "Personal" is defined here as any device which is not issued/sanctioned by the CBSA for use strictly within the CBSA.
- Connect any other portable device to the CBSA Networked Workstation, from a trusted or untrusted source, before assessing if any potential threats exist.
    - An example of a trusted source is considered to be received from any Government of Canada entity.
    - Examples of an untrusted source would be: course material provided by external training, a traveller's portable storage device, information provided at trade shows.
    - Once it is determined if the devices can safely be connected to the CBSA network, the use of these devices is approved for one way transfer only (saving information from the device to the CBSA network).
- Connect a CBSA issued device to the CBSA Network that has been connected outside of the Government of Canada environment, before assessing if any potential threats exist.
    - For example, a CBSA portable device was used to transfer information to a third party vendor of CBSA.
- Connect any other type of device, such as a personal communication device for the purposes of charging (including, but not limited to, smart phones, music players, e-cigarettes, USB powered lights, etc).
- Use portable devices to transfer information between networks of different classifications, without consulting with CBSA Information Security.
- Use portable devices as permanent and/or single document repositories to store CBSA information.

Existing guidance remains unchanged when transporting a portable device such as a BlackBerry or laptop with CBSA information stored on it. The bearer must keep it under their constant control and possession at all times.

## 4. Management of Portable Data Storage Devices

Each CBSA directorate is required to label, log, track and securely store portable data storage devices. It is recommended that an inventory list be maintained by the same individuals responsible for ordering and safe-keeping the devices (ex. Administrative assistants and/or supervisors). A manager's written consent must be provided before a portable storage device can be issued, and the device must be returned to the inventory and stored in a secure, locked cabinet. Refer to Appendix 1 for an example of a tracking sheet/inventory.



CBSA will maintain records of the portable devices issued within the organization. At a minimum, the record will contain a unique identifier (such as a serial number) of the device, the assignee name, the date of assignment, and the purpose and highest level of security classification of the information that is permitted to be stored on the device.
Portable devices must be labelled to indicate the highest classification level of information that has been stored on the device. CBSA must use an indirect coding system that is not immediately recognizable to the general public.

If any employee/section has a specific business requirement(s) to burn CD's and DVD's, they will be required to provide a complete business rationale for the exemption to the Information Security Section. Please note: computers not connected to the CBSA network (such as standalones, CCTV stations, etc.) will be unaffected by the CD/DVD burning restrictions.

Directorates are responsible for:

- The management of a centralized inventory list.
- Labelling, issuing, tracking, and collecting all portable devices.
- Ensuring all employees issued a portable device have read this procedure and understand their responsibilities.
- Ensuring all portable devices are issued for **temporary** use, the devices are returned to the inventory when no longer needed and stored securely.
- Ensuring all portable devices are stored according to the highest level of information ever stored on the device, even if the storage devices has been cleared/wiped.
- Ensuring portable devices are destroyed appropriately, when they are no longer required or no longer performing their intended function; as well as retain a certificate of destruction for all portable storage devices, whether destroyed internally, or performed by an external service provider.
- Clearing all directorate portable devices when returned to inventory, and storing securely until re-issued. See USB Key - Security - Formatting and reassigning a USB key.
- Reporting lost/stolen devices or employee non-compliance to the Departmental Security Officer (DSO).

HQ/Regional Security offices are responsible for:

- Performing a verification function to ensure that centralized inventory lists are maintained and updated in each Directorate.
- Sharing the results from these audits with the Information Security Section on request.



## 5. Handling, Storage, and Transmittal

Portable devices must be properly secured at all times as appropriate to the highest level of security classification of the information, currently or previously, stored on it. For example, if a device currently stores non-classified information, but contained Protected B information previously, it must be treated as Protected B. Similarly, if a device is ever used to store Secret information, it can never be connected to the Protected B Network again.

Password or biometric controlled portable devices and encryption of the CBSA information stored on them supplements but do not replace physical security procedures.

Please consult the CBSA Security Volume and the RCMP standards for the storage of material at the various classification levels.

Specific requirements related to physical security and security containers can be found in the TBS Operational Security Standard on Physical Security (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329 ) and the Royal Canadian Mounted Police (RCMP) guides G1-001, Security Equipment Guide (http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm ) and G1-009, Transport and Transmittal of Protected and Classified Information (http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-eng.htm ).

## 6. Clearing and Disposal

Clearing is the process of erasing stored information from portable data storage devices in a manner that allows it to be re-used within an equivalent security environment.

Clearing must be adequate to prevent information recovery using readily available tools capable of recovering deleted information. Simply deleting or erasing the files or reformatting does not clear the portable data storage device, because commands such as undelete or un-format may permit the recovery of the information.

Additionally, even when appropriately cleared, it may still be possible to recover data from the device when using specialized IT utilities or laboratory techniques. For this reason, cleared portable data storage devices must be retained within security environments appropriate to the highest level of information that the device once contained, and the device cannot be considered for declassification.

Individual users must return portable data storage devices to the CBSA for destruction and disposal. CBSA must retain a certificate of destruction for all portable storage devices, whether destroyed internally, or performed by an external service provider. For information on the proper disposal of data storage devices, please see the Standard for the Sanitization or Destruction of Information Assets, and contact Regional or Headquarters Security.



Clearing and disposal must be in accordance with CSEC's ITSG-06, Clearing and Declassifying Electronic Data Storage Devices.

## 7. Other USB Devices

Above and beyond approved CBSA portable devices, there are numerous new technologies which make use of the USB interface for various reasons such as charging, syncing, data transfer, etc. Each of these may have associated attack vectors which are changing and being exploited every day at an ever increasing rate. Unless issued by CBSA, these devices should NEVER be plugged into a CBSA workstation, nor be used in conjunction with any CBSA issued device. This may significantly increase the risk for the Agency to an unacceptable/unknown level.

## 8. Exemptions

Only with formal Agency approval (Departmental Security Officer) are the following exceptions for the use of unauthorized portable devices permissible:

- Connecting an unauthorized device to CBSA IT networks for the purpose of one-way transfers of information from the device to CBSA IT networks;
- Storing CBSA information on an unauthorized device;
- Storing unencrypted CBSA information on a non-password or non-biometric controlled portable device;
- Connecting and/or using a portable device to the CBSA secret network.

Currently, within CBSA all USB ports are locked down on the CBSA Secret Network. The Departmental Security Officer (DSO) will work with groups to determine information transfer solutions on a case by case basis.

## 9. Reporting Security Incidents

CBSA employees (including contractors, students, etc.) are responsible to report loss or theft of portable devices immediately to Security and Professional Standards Directorate (SPSD) within 24 hours of the incident. There will be a requirement to fill in a Security Incident Report, as per the Standard for Security Incident Reporting.

Even the best policies and practices cannot eliminate risk entirely. Mistakes and errors will inevitably occur. All employees at all levels should be aware to report any mistakes/errors with respect to USB devices to Security and Professional Standards and be prepared to accurately document any incident.



In accordance with TBS Guidelines for Privacy Breaches, CBSA must report any real or suspected loss or theft of portable devices, containing personal information, to:

- Treasury Board Secretariat / Chief Information Officer Branch;
- Access to Information and Privacy officials; and
- The Office of the Privacy Commissioner

## 10. References

**Secure use of portable data storage devices within the Government of Canada:**
http://www.tbs-sct.gc.ca/it-ti/itpin-ampti/2014-01-eng.asp

**CBSA Security Volume:**
http://atlas/cb-dgc/pol/cm-mc/sv-vs/index_eng.asp

**Access to Information and Privacy:**
http://www.tbs-sct.gc.ca/atip-aiprp/index-eng.asp

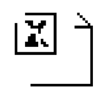
**Treasury Board Guidelines for Privacy Breaches:**
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154&section=text

## 11. Enquiries

| Office Responsible | Contact Information |
|---|---|
| **Comptrollership Branch**<br>Security and Professional Standards Directorate | **E-mail**:<br>Information_Security-Securite_de_linformation@cbsa-asfc.gc.ca |
| **Innovation, Science and Technology Branch** | **E-mail**: CBSA/ASFC-IT SECURITY/SECURITE TI<br>**Intranet**: IT Security |



# 12. Appendix 1 - Inventory Template



Inventory Template.xlsx



Agence des services frontaliers du Canada | Canada Border Services Agency



# Procédures pour l'utilisation des dispositifs de stockage de données portatifs à l'ASFC



PROTECTION • SERVICE • INTÉGRITÉ





# Table des matières



Ces procédures entre en vigueur le 22 décembre 2015.

## 1. Objectif

Les procédures suivantes visent à mettre en évidence les responsabilités des auteurs et des destinataires quant à la manipulation appropriée de l'information et des biens en ce qui concerne l'utilisation des dispositifs de stockage de données portatifs (ci-après appelés « dispositifs portatifs »). La protection des biens d'information est le principal objectif de la sécurité de l'information. Il est important d'adopter des comportements sécuritaires en matière d'informatique afin de réduire les occurrences de vol, de perte ou de mauvaise utilisation des biens d'information du gouvernement. Les infractions à la sécurité de l'information ou les pertes de biens d'information peuvent avoir des conséquences graves, selon la sensibilité et la valeur de l'information et l'ampleur de l'infraction.

**Ces procédures s'appliquent à toute l'information ou à tout type d'information que manipulent les fonctionnaires ou les sous-traitants de l'ASFC et qui est transmis ou stocké au moyen de dispositifs portatifs.**

Un autre objectif de ces procédures est l'établissement de normes minimales concernant l'utilisation et la protection des données transmises ou stockées au moyen de dispositifs portatifs (clés USB, appareils à mémoire flash, CD/DVD, disques durs externes, etc.). Les dispositifs portatifs peuvent être très utiles dans le cadre des opérations de l'ASFC; toutefois, en raison de leur petite taille, ils peuvent être facilement perdus ou volés, ce qui peut entraîner des infractions à la sécurité. Les dispositifs portatifs ont une capacité de stockage de plus en plus grande et peuvent contenir de grandes quantités de fichiers et de données. Les assistants numériques personnels, les BlackBerry, les iPod et les autres lecteurs multimédias peuvent stocker des fichiers et entrent dans la catégorie des dispositifs portatifs.

Le fait que ces dispositifs soient très répandus à l'ASFC cause d'importants problèmes de soutien et des risques sur le plan de la sécurité. Bien que le coût de remplacement des dispositifs soit relativement insignifiant, de plus en plus d'utilisateurs enregistrent des données sensibles dans ces appareils, ce qui crée un risque de fuite de données. De plus, l'utilisation des dispositifs portatifs peut entraîner un certain nombre de menaces pour la sécurité du réseau de l'ASFC, comme la propagation de logiciels malveillants, de virus ou de vers.



## 2. Conséquences des infractions

**Les conséquences des infractions peuvent comprendre, sans toutefois s'y limiter :**

- la divulgation de renseignements personnels ou de données opérationnelles;
- la propagation possiblement non intentionnelle de logiciels malveillants, de virus, de logiciels espions et d'autres types de logiciels indésirables;
- l'interruption de la capacité du gouvernement de fournir des services;
- des pertes financières liées aux mesures à prendre pour corriger la situation;
- des menaces pour la sécurité publique ou pour la santé et le bien-être de certaines personnes;
- des poursuites en justice;
- l'érosion de la confiance du public à l'égard du gouvernement.

**Sujets de préoccupation**

Le principal sujet de préoccupation est le risque que les dispositifs portatifs soient perdus, volés ou utilisés de façon abusive et que des données appartenant au gouvernement soient divulguées, modifiées ou détruites de façon inappropriée.

*De nombreux facteurs contribuent à cette préoccupation :*

- L'utilisation de dispositifs personnels ou non autorisés peut mener à des infractions à la sécurité (dispositifs de stockage USB personnels, lecteurs de fichiers musicaux/vidéos, etc.).
- La petite taille des dispositifs portatifs rend ceux-ci plus susceptibles d'être perdus ou volés.
- L'absence de processus de signalement rapide de dispositifs perdus, volés ou endommagés augmente le risque que l'information soit divulguée, modifiée ou détruite de façon inappropriée.
- Des dispositifs non sécurisés ou mal sécurisés accroissent les risques pour la sécurité et la confidentialité de l'information et des ressources documentaires.
- Les dispositifs portatifs ont d'importantes capacités de stockage, ce qui peut mener au vol de grandes quantités de données ou de programmes.
- Des logiciels malveillants et des virus peuvent être propagés sur ces dispositifs à partir de nombreuses sources (cadeaux lors des salons professionnels, inspection des dispositifs à divers postes frontaliers, dispositifs non certifiés connectés à des ordinateurs, etc.). La liste des sources possibles est longue et bien remplie.
- Des dispositifs portatifs peuvent être utilisés sans qu'il y ait d'outils à l'échelle de l'entreprise pour gérer leur utilisation et leur élimination.
- Il se peut que les mesures de sécurité comme le cryptage ne soient pas utilisées lorsque des dispositifs portatifs servent à transporter des données de l'ASFC.



# 3. Utilisation des dispositifs de stockage de données portatifs à l'ASFC

Afin de limiter les risques pour l'Agence, les employés de l'ASFC (ceci comprend les employés permanents, nommés pour une période déterminée, occasionnels et à temps partiel, le personnel à contrat et le personnel d'agences privées, ainsi que les personnes en détachement ou en affectation à l'ASFC, y compris les étudiants) doivent **toujours** :

- éviter d'utiliser des dispositifs portatifs dans la mesure du possible, ou sinon en limiter l'utilisation au maximum;
- utiliser les dispositifs portatifs uniquement pour stocker temporairement l'information de l'ASFC;
- utiliser uniquement les dispositifs attribués et répertoriés par l'ASFC;
- veiller à ce que tous les dispositifs portatifs soient protégés par mot de passe ou identificateur biométrique et à ce que l'information de l'ASFC qu'ils renferment soit cryptée;
- veiller à ce que les dispositifs portatifs soient manipulés, entreposés et transportés conformément au niveau de classification des données;
- retourner tous les dispositifs portatifs à l'inventaire une fois que l'exigence relative à l'utilisation temporaire est satisfaite (voir section 4);
- signaler immédiatement la perte ou le vol d'un dispositif de stockage portatif (voir section 9).

Les employés de l'ASFC ne doivent **jamais** :

- utiliser un dispositif portatif « personnel » pour stocker de l'information de l'ASFC, ni connecter un dispositif personnel au réseau de l'ASFC (l'utilisation de dispositifs portatifs « personnels » est interdite);
  - le terme « personnel » signifie tout appareil qui n'est pas autorisé/attribué par l'ASFC pour une utilisation strictement limitée à l'ASFC;
- connecter tout autre dispositif portatif provenant d'une source fiable ou non fiable à un poste de travail connecté au réseau de l'ASFC avant d'évaluer si elles contiennent des menaces potentielles;
  - du matériel reçu d'un entité du Gouvernement du Canada est un exemple de source fiable;
  - du matériel de cours fourni lors d'une formation externe, un dispositif de stockage portatif appartenant à un voyageur, de l'information obtenu à des salons professionnel sont des exemples de sources non fiables;
  - une fois qu'il aura été déterminé que les dispositifs peuvent être connectés au réseau de l'ASFC de façon sécuritaire, ces dispositifs peuvent être utilisés pour effectuer un <u>transfert unidirectionnel</u> seulement (sauvegarder l'information dans le réseau de l'ASFC à partir du dispositif);
- connecter au réseau de l'ASFC un dispositif portatif remis par l'ASFC qui a été connecté à l'extérieur de l'environnement du Gouvernement du Canada avant d'évaluer si elles contiennent des menaces potentielles;



  - par exemple, un dispositif portatif de l'ASFC a été utilisé pour transmettre de l'information à un fournisseur indépendant de l'ASFC;
- connecter tout autre type de dispositif, comme un appareil de communication personnel, dans le but de le recharger (téléphones intelligents, lecteurs de fichiers musicaux, cigarettes électroniques, dispositifs d'éclairage USB, etc.);
- utiliser des dispositifs portatifs pour transférer de l'information entre des réseaux de classifications différentes sans consulter préalablement la Sécurité de l'information de l'ASFC;
- utiliser des dispositifs portatifs comme dépôt de documents unique ou permanent pour stocker de l'information de l'ASFC.

Les directives actuellement en vigueur demeurent inchangées pour ce qui est du transport de dispositifs portatifs tels qu'un BlackBerry ou un ordinateur portatif contenant de l'information de l'ASFC. La personne en charge de tels dispositifs doit les surveiller constamment et les avoir en sa possession en tout temps.

## 4. Gestion des dispositifs de stockage de données portatifs

Chaque direction de l'ASFC est tenue d'étiqueter, de répertorier, de suivre et d'entreposer de manière sécuritaire les dispositifs de stockage de données portatifs. On recommande que les mêmes personnes qui sont chargées de commander les dispositifs et d'en assurer la sécurité (p. ex. adjoints administratifs ou superviseurs) tiennent un inventaire de ces dispositifs. La permission écrite d'un gestionnaire est requise avant qu'un dispositif de stockage de données portatif puisse être remis, et le dispositif doit être retourné à l'inventaire et entreposé dans une armoire sécurisée et verrouillée. L'annexe 1 contient un exemple de formulaire de suivi/d'inventaire.

L'ASFC tiendra des registres des dispositifs de stockage portatifs fournis au sein de l'organisation. Le registre indiquera à tout le moins l'identificateur unique (comme le numéro de série) de chaque dispositif, le nom du détenteur, la date d'attribution, la raison de l'attribution et le plus haut niveau de classification de sécurité de l'information qu'il est permis de sauvegarder sur le dispositif. Les dispositifs portatifs doivent être étiquetés pour indiquer le plus haut niveau de classification de l'information qui y est stockée. L'ASFC doit utiliser un système de codage indirect qui n'est pas immédiatement reconnaissable par le grand public.

Si un employé ou une section doit faire graver des CD et des DVD pour combler des besoins opérationnels particuliers, une justification complète de l'exemption doit être fournie à la Section de la sécurité de l'information. Veillez noter que les restrictions pour faire graver des concernant la gravure de CD et des de DVD ne concernent pas les ordinateurs qui ne sont pas connectées au sur le réseau de l'ASFC (tel que les ordinateurs non connectés, les stations TVCF, etc.).

Les directions sont responsables :

- de gérer un inventaire centralisé;



- d'étiqueter, d'attribuer, de suivre et de récupérer tous les dispositifs portatifs;
- de faire en sorte que tous les employés à qui on a attribué un dispositif portatif aient pris connaissance de la présente procédure et comprennent leurs responsabilités;
- de veiller à ce que tous les dispositifs portatifs servent **temporairement**, soient retournés à l'inventaire lorsqu'on n'en a plus besoin et soient entreposés en toute sécurité;
- de veiller à ce que tous les dispositifs portatifs soient entreposés conformément au niveau de classification le plus élevé de toute l'information qui a été stockée sur chaque dispositif, même si celui-ci a été vidé de son contenu/formaté;
- de faire en sorte que les dispositifs portatifs soient détruits de manière appropriée lorsqu'on n'en a plus besoin ou lorsqu'ils ne remplissent plus leur fonction;
- de vider de leur contenu tous les dispositifs portatifs qui sont retournés à l'inventaire et de les entreposer en toute sécurité jusqu'à ce qu'ils soient attribués de nouveau. Voir Clé USB - Sécurité - Formater et réattribuer une clé USB ;
- de signaler les dispositifs perdus ou volés et tout manquement aux règles de la part des employés à l'agent de sécurité du ministère (ASM).

L'AC / les bureaux régionaux de sécurité doivent :

- procéder à une vérification pour s'assurer que chaque direction maintien et mets à jour des listes d'inventaire centralisées;
- transmettre, sur demande, les conclusions de ces vérifications à la Section de la sécurité de l'information.

## 5. Manipulation, entreposage et transmission

Les dispositifs portatifs doivent être bien protégés en tout temps selon le plus haut niveau de classification de sécurité de l'information qui y est ou qui y était stockée. Par exemple, si de l'information non classifiée est stockée dans un dispositif portatif sur lequel de l'information Protégé B a déjà été stockée, le dispositif doit être traité au niveau Protégé B. De la même façon, si de l'information secrète est stockée dans un dispositif, celui-ci ne doit plus jamais être connecté au réseau protégé B.

Le contrôle des dispositifs portatifs au moyen d'un mot de passe ou d'un identificateur biométrique et le cryptage de l'information de l'ASFC qui y est sauvegardée complètent les procédures de sécurité physique sans toutefois les remplacer.
Veuillez consulter le Volume de sécurité de l'ASFC et les normes de la GRC concernant l'entreposage du matériel en fonction des différents niveaux de classification.

Les exigences précises concernant la sécurité physique et les coffres de sécurité se trouvent dans la Norme opérationnelle sur la sécurité matérielle du SCT (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329) et les guides G1-001, Guide d'équipement de sécurité (http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm), et G1-009, Transport et transmission de renseignements protégés ou classifiés (http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-fra.htm) de la Gendarmerie royale du Canada (GRC).



## 6. Effacement et élimination

L'effacement est le processus qui consiste à effacer l'information qui est sauvegardée sur des dispositifs de stockage de données portatifs d'une manière permettant de la réutiliser dans un environnement de sécurité équivalent.

L'effacement doit pouvoir empêcher toute récupération des données à l'aide des outils habituellement disponibles pour récupérer de l'information supprimée. La suppression ou l'effacement des données ou le formatage d'un disque n'efface pas de façon permanente les données car des commandes comme « annulation de la suppression » ou « annulation du formatage » peuvent permettre la récupération des données.

De plus, même lorsque l'effacement est fait correctement, il peut être possible de récupérer les données du dispositif au moyen d'outils de TI ou de techniques de laboratoire spécialisés. Pour cette raison, les dispositifs de stockage de données portatifs effacés doivent être conservés dans un environnement dont le niveau de sécurité correspond au niveau de sécurité le plus élevé de l'information qui y était sauvegardée, et ils ne doivent pas faire l'objet d'une déclassification.

Chaque utilisateur doit remettre les dispositifs de stockage de données portatifs à l'ASFC pour que ceux-ci soient éliminés ou détruits. L'ASFC doit conserver un certificat de destruction pour chaque dispositif de stockage de données portatif, que la destruction ait été effectuée par l'ASFC ou par un fournisseur de service externe. Pour obtenir des renseignements sur l'élimination appropriée des dispositifs de stockage de données portatifs, veuillez consulter la Norme pour le nettoyage ou la destruction des ressources d'information et communiquer avec l'équipe de sécurité de votre région ou de l'Administration centrale.

L'effacement et l'élimination doivent être effectués conformément aux dispositions énoncées dans le document ITSG-06 du CST, Effacement et déclassification des supports d'information électroniques.

## 7. Autres dispositifs USB

En plus des dispositifs portatifs approuvés par l'ASFC, de nombreuses autres technologies utilisent l'interface USB pour diverses raisons, comme la recharge, la synchronisation, le transfert de données, etc. Chacune de ses fonctions peut être associée à des vecteurs d'attaque qui évoluent et sont exploités chaque jour à un rythme de plus en plus rapide. À l'exception de ceux qui ont été attribués par l'ASFC, ces dispositifs ne doivent JAMAIS être connectés à un poste de travail de l'ASFC ni être utilisés avec un autre dispositif attribué par l'ASFC. Agir ainsi peut présenter un risque de niveau inacceptable/inconnu pour l'Agence.



## 8. Exemptions

Les exceptions suivantes quant à l'utilisation de dispositifs portatifs non autorisés sont permises avec l'autorisation officielle de l'Agence (agent de sécurité du ministère) seulement :

- connexion d'un dispositif non autorisé aux réseaux de TI de l'ASFC aux fins de transfert unidirectionnel de données du dispositif vers les réseaux de TI de l'ASFC;
- stockage d'information de l'ASFC sur un dispositif non autorisé;
- stockage d'information de l'ASFC non cryptée sur un dispositif qui n'est pas protégé par un mot de passe ou un identificateur biométrique;
- connexion ou utilisation d'un dispositif portatif sur le réseau secret de l'ASFC.

À l'heure actuelle, à l'ASFC, tous les ports USB sont verrouillés sur le réseau secret de l'Agence. L'agent de sécurité du ministère (ASM) collaborera avec les groupes pour trouver des solutions pour le transfert d'information au cas par cas.

## 9. Signalement des incidents de sécurité

Les employés de l'ASFC (y compris le personnel à contrat, les étudiants, etc.) ont la responsabilité de signaler la perte ou le vol d'un dispositif portatif à la Direction de la sécurité et des normes professionnelles (DSNP) dans les 24 heures suivant l'incident. Conformément à la norme de signalement des incidents de sécurité, il faut remplir un rapport d'incident de sécurité.

Même les meilleures politiques et pratiques ne peuvent éliminer complètement les risques. Des erreurs vont inévitablement se produire. Tous les employés à tous les niveaux doivent savoir qu'ils doivent signaler toute erreur relativement aux dispositifs USB à la Direction de la sécurité et des normes professionnelles et être prêts à documenter avec précision tout incident.
Conformément aux Lignes directrices sur les atteintes à la vie privée du SCT, l'ASFC doit signaler toute perte et tout vol réels ou présumés de dispositifs portatifs contenant des renseignements personnels aux personnes et organismes suivants :

- Secrétariat du Conseil du Trésor / Direction du dirigeant principal de l'information;
- agents affectés à la protection de la vie privée et à l'accès à l'information;
- Commissariat à la protection de la vie privée.



•

## 10. Références

**Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada :** http://www.tbs-sct.gc.ca/it-ti/itpin-ampti/2014-01-fra.asp

**Volume de sécurité de l'ASFC :**
http://atlas/cb-dgc/pol/cm-mc/sv-vs/index_fra.asp

**Accès à l'information et protection des renseignements personnels :**
http://www.tbs-sct.gc.ca/atip-aiprp/index-fra.asp

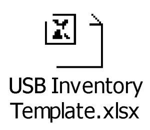
**Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor :**
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26154&section=text



## 11. Demandes de renseignements

| Bureau responsable | Coordonnées |
|---|---|
| **Direction générale du contrôle**<br>Direction de la sécurité et des normes professionnelles | **Courriel :** Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca |
| **Direction générale de l'innovation, des sciences et de la technologie** | **Courriel :** CBSA/ASFC-IT SECURITY/SECURITE TI<br>**Intranet :** Sécurité des TI |

## 12. Annexe 1 – Gabarit pour l'inventaire



USB Inventory Template.xlsx

Canada Border Services Agency | Agence des services frontaliers du Canada



# Guidelines for Protection of Information Assets - Social Engineering Awareness

Information Security

Infrastructure and Information Security Division

Security and Professional Standards Directorate

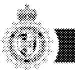
16 December 2014

PROTECTION • SERVICE • INTEGRITY





## Contents



# OBJECTIVE

This guideline intends to explain social engineering to CBSA employees and provides means to recognize and counter social engineering attempts.

# WHAT IS SOCIAL ENGINEERING?

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging sensitive information.

# RECOGNIZING SOCIAL ENGINEERING

There are many types of Social engineering attacks which CBSA users should be at least aware of these types of attacks.

## Pretexting

Pretexting is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.

An intricate lie is often used to establish legitimacy in the mind of a target. Frequently an elaborate story often involves prior research or setup and the use of information for impersonation (e.g., date of birth, Social Insurance Number, last bill amount, etc.).

Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, clergy, insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the targeted victim. The pretexter must simply prepare answers to questions that might be asked by the victim. In some cases, all that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet to create a credible (pretext) scenario.

This technique can be used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives. The information can then be used to establish even greater legitimacy under tougher questioning with a manager, e.g., to make account changes, get specific balances, etc.

## Diversion theft

Diversion theft is a "con" exercised by professional thieves, normally against a transport or courier company. The objective is to persuade the persons responsible for the legitimate delivery of goods that these goods are requested elsewhere.







### Phishing

Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business, such as a bank, or credit card company, requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate, with company logos and content, and has a form requesting everything from a home address to an ATM card's PIN.

### Malicious and SPAM emails

Malicious and SPAM emails are tailored to entice the reader to open them. Unsuspecting users may be tempted to open malicious email attachments or follow embedded links to malicious websites – either action could lead to a compromise of sensitive information. These campaigns are becoming increasingly tailored and appear to be credible. Similar to phishing, malicious emails often appear to be from someone the reader knows, such as their employer, colleague or friend. Some even have convincing-looking commercial logos and signatures and target a specific personal interest or a subject matter relevant to their work. Some malicious websites can be equally convincing. They can masquerade as a legitimate site used by an individual, such as their personal banking website, in order to mislead them into revealing personal or corporate information.

### Quid pro quo

Quid pro quo means something for something. For instance an attacker calls random numbers at a company, claiming to be calling back from technical support. Eventually this person will hit someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker access or launch malicious software designed to damage or do other unwanted actions within a computer system.

### Tailgating

An attacker, seeking entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the door open for the attacker. The legitimate person may fail to ask for identification for any number of reasons, or may accept an assertion that the attacker has forgotten or lost the appropriate identity token. The attacker may also present a fake identity token.

## COUNTERING SOCIAL ENGINEERING ATTACKS

### Organizational Contribution

To counter social engineering attacks, CBSA employs the following measures:

- Provides information security management policy instruments (policy, standards, guidelines) to specify when/where/why/how sensitive information should be handled;
- Provides Security Awareness training in support of information security;
- Provides security training to employees that is relevant to their position;
- Offers Regional Security Office and Security and Professional Standards Directorate assistance/guidance to CBSA users with identifying which information is sensitive and







evaluating its exposure to social engineering and breakdowns in security systems (building, computer system, etc.);
- Performs unannounced, periodic tests of security protocols;
- Regularly reviews and continuously improves the security program; and
- Provides software (e.g. anti-virus, encryption) and equipment (e.g. briefcases, locked cabinets, secure facsimile machines) to enable CBSA users to securely handle their information.

### Individual Contribution

The integrity of CBSA employees is the best line of defense for protecting sensitive information. CBSA users must all contribute to social engineering countering, by:

- Developing and maintaining awareness of social engineering attacks and countermeasures;
- Taking the online security awareness training within 10 days from the date of employment and every 2 years thereafter;
- Requesting the identity of any requester if social engineering is suspected before continuing the conversation or replying by email, fax or online;
- Stopping the conversation and following security incident reporting procedures if the identity of a requester cannot be promptly verified;
- Knowing who to contact for security guidance and for security incident reporting; and
- Recognizing that they are an important part of the security of the CBSA.

## REFERENCES

- Wikipedia – Social Engineering (Security) - http://en.wikipedia.org/wiki/Social_engineering_(security)






Agence des services frontaliers du Canada | Canada Border Services Agency



# Lignes directrices en matière de protection des ressources d'information – Sensibilisation à l'ingénierie sociale

Sécurité de l'information

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

Le 27 janvier 2015

PROTECTION • SERVICE • INTÉGRITÉ





# Table des matières



# OBJECTIF

Ces lignes directrices ont pour objet d'expliquer l'ingénierie sociale aux employés de l'Agence des services frontaliers du Canada (ASFC), et de fournir des moyens de reconnaître et de contrer les tentatives d'ingénierie sociale.

# EN QUOI CONSISTE L'INGÉNIERIE SOCIALE?

L'ingénierie sociale, selon le contexte de la sécurité de l'information, des ordinateurs, est la pratique consistant à obtenir ou à tenter d'obtenir des données protégées en dupant une personne pour qu'elle divulgue des renseignements protégés. Les ingénieurs sociaux exploitent la tendance naturelle des gens à faire confiance. Les victimes de l'ingénierie sociale peuvent être dupées pour divulguer des renseignements qui, sans le savoir, peuvent être utilisés pour attaquer un réseau d'ordinateurs ou pour utiliser, de diverses façons, de l'information à première vue innocente. En général, cette méthode de persuasion se rapporte à la manipulation psychologique de personnes pour poser des gestes ou divulguer des renseignements de nature délicate.

# RECONNAÎTRE L'INGÉNIERIE SOCIALE

Il existe de nombreux types d'attaque d'ingénierie sociale auxquels les utilisateurs de l'ASFC doivent à tout le moins être sensibilisés.

## Faux-semblant

Cette expression désigne la création et l'utilisation d'un scénario inventé pour susciter l'intérêt d'une victime ciblée de manière à accroître les chances que la victime divulgue de l'information ou pose des gestes malgré les réticences qu'elle aurait à le faire normalement, ou dans le cas de l'ASFC, divulgue de l'information ou pose des gestes contraires au Code de conduite de l'ASFC ou au Code criminel du Canada.

Un mensonge complexe est souvent utilisé pour établir la légitimité dans l'esprit de la cible. Un récit élaboré englobe souvent une mise en scène et l'utilisation de renseignements obtenus au préalable, notamment aux fins d'usurpation d'identité (p. ex. date de naissance, numéro d'assurance sociale, montant de la dernière facture).

Le faux-semblant peut également être utilisé pour personnifier des collègues, des policiers, des représentants bancaires, des autorités fiscales, des membres du clergé, des enquêteurs de compagnie d'assurances, ou toute autre personne pouvant sembler détenir un pouvoir ou avoir un droit de savoir dans l'esprit de la victime ciblée. Le fraudeur doit simplement préparer des réponses aux questions susceptibles d'être posées par la victime. Dans certains cas, l'auteur du faux-semblant n'a besoin que de prendre une voix faisant autorité et un ton sincère et à être en mesure de réagir rapidement pour créer un scénario crédible (prétexte).







Cette technique peut être utilisée pour tromper une entreprise afin de l'amener à divulguer de l'information sur ses clients. Les détectives privés peuvent également s'en servir pour obtenir des relevés téléphoniques, des relevés de services publics, des dossiers bancaires et d'autres documents, directement auprès des préposés au service des entreprises. L'information peut ensuite être utilisée pour renforcer la légitimité quand le stratagème est utilisé de façon plus poussée auprès d'un gestionnaire (p. ex. pour apporter des modifications dans un compte ou obtenir des soldes précis). Il y a de nombreuses raisons de vouloir obtenir des renseignements des employés de l'ASFC ou à leur sujet comme la vengeance, la trahison, les gains personnels, les activités terroristes, l'extorsion.

# Vol par détournement

Le vol par détournement est une arnaque que des voleurs chevronnés utilisent, habituellement contre des entreprises de transport ou de messagerie. L'objectif consiste à convaincre les personnes chargées de la livraison légitime de biens que ceux-ci sont demandés ailleurs.

# Hameçonnage

L'hameçonnage est une technique qui consiste à obtenir frauduleusement des renseignements confidentiels. Habituellement, l'hameçonneur envoie un courriel qui semble provenir d'une d'entreprise légitime, comme une banque ou une société de carte de crédit, et qui demande de transmettre certains renseignements sous peine de conséquences désastreuses. Le courriel contient généralement un lien menant vers un site frauduleux qui paraît légitime (logo, contenu), ainsi qu'un formulaire où inscrire divers renseignements (adresse à domicile, NIP).

# Courriels malveillants et pourriels

Les courriels malveillants et les pourriels sont adaptés afin d'inciter le destinataire à les ouvrir. Les utilisateurs peu méfiants peuvent être tentés d'ouvrir des pièces jointes contenues dans les courriels malveillants ou de cliquer sur des liens intégrés menant à des sites Web malveillants; ces deux gestes sont susceptibles de compromettre la sécurité des renseignements de nature délicate. Ces campagnes sont de mieux en mieux adaptées et semblent crédibles. À l'instar de l'hameçonnage, les courriels malveillants semblent souvent provenir d'un expéditeur connu de la cible, comme son employeur, un collègue ou un ami. Certains auteurs de ces types de courriels ont des logos et signatures d'entreprise convaincants, et ciblent un intérêt personnel particulier de la victime ou un sujet pertinent par rapport au travail de celle-ci. Certains sites Web malveillants peuvent être tout aussi convaincants. Ils peuvent se faire passer pour un site légitime utilisé par la victime (p. ex. site Web du compte bancaire personnel) afin de l'amener frauduleusement à révéler des renseignements personnels ou organisationnels.

# Contrepartie

Par « contrepartie », on entend le principe du donnant-donnant. À titre d'exemple, un pirate compose des numéros au hasard au sein d'une entreprise en se faisant passer pour un employé de soutien technique qui répond à un appel de service. Le pirate tombera éventuellement sur une personne qui a un problème réel et qui sera reconnaissante qu'on la rappelle pour lui offrir de l'aide. Le pirate « aidera » la personne à régler son problème et, en faisant cela, obtiendra les commandes liées au type d'utilisateur qui lui donneront accès au







système informatique ou qui lui permettront de lancer un logiciel malveillant conçu pour endommager le système ou y effectuer des opérations non autorisées.

## Passage en double

Un pirate qui cherche à s'introduire dans une zone d'accès restreint protégée par un contrôle électronique de l'accès sans personnel de surveillance (p. ex. avec une carte RFID [identification par radiofréquence]) marche simplement derrière une personne qui a un accès légitime. Par simple courtoisie, la personne qui a un accès légitime tient habituellement la porte ouverte pour la personne qui la suit (le pirate). Pour diverses raisons, la personne qui a un accès légitime peut omettre de demander à l'autre personne de s'identifier ou peut accepter l'explication fournie par celle-ci, à savoir qu'elle a oublié ou perdu sa pièce d'identité. Le pirate peut également lui présenter une fausse pièce d'identité.

# CONTRER LES ATTAQUES D'INGÉNIERIE SOCIALE

## Contribution à l'échelle de l'organisation

Pour contrer les attaques d'ingénierie sociale, l'ASFC :

- fournit des instruments stratégiques de gestion de la sécurité de l'information (politique, normes, lignes directrices) afin de préciser le moment et le lieu où l'information de nature délicate devrait être traitée, ainsi que la raison pour laquelle elle devrait être traitée et la façon dont elle devrait l'être;
- offre une formation sur la sensibilisation à la sécurité à l'appui de la sécurité de l'information;
- fournit aux employés une formation sur la sécurité liée aux exigences de leur poste;
- offre l'aide et l'orientation du bureau régional de sécurité et de la Direction de la sécurité et des normes professionnelles aux utilisateurs de l'ASFC, afin de leur permettre de cerner les renseignements de nature délicate, et d'évaluer l'exposition de ceux-ci à l'ingénierie sociale et leur vulnérabilité en cas de panne des systèmes de sécurité (immeuble, système informatique, etc.);
- vérifie périodiquement et de façon non annoncée le respect des protocoles de sécurité;
- examine régulièrement et améliore continuellement le programme de sécurité;
- fournit des logiciels (p. ex. antivirus, chiffrement) et de l'équipement (p. ex. serviettes, classeurs verrouillés, télécopieurs sécurisés) aux utilisateurs de l'ASFC afin de leur permettre de voir à la sécurité de l'information en leur possession.







# Contribution individuelle

L'intégrité des employés de l'ASFC représente le meilleur moyen de défense en vue de protéger les renseignements de nature délicate. Les utilisateurs de l'ASFC doivent tous participer à la lutte contre l'ingénierie sociale en :

- restant sensibilisés aux attaques d'ingénierie sociale et aux mesures de prévention de celles-ci;
- suivant la formation en ligne sur la sensibilisation à la sécurité dans les 10 jours suivant la date d'emploi et tous les deux ans par la suite;
- exigeant à tout demandeur de s'identifier, s'ils suspectent une attaque d'ingénierie sociale, avant de continuer la conversation ou de répondre par courriel, par télécopieur ou en ligne;
- mettant fin à la conversation et en suivant les procédures de signalement des incidents de sécurité si l'identité d'un demandeur ne peut être vérifiée dans les plus brefs délais;
- sachant avec qui communiquer pour obtenir des avis en matière de sécurité et pour signaler des incidents de sécurité;
- reconnaissant qu'ils ont un rôle important à jouer pour protéger l'ASFC.
- reconnaître que tous les employés (temps plein, temps partiel, agents contractuels, étudiants) constituent une importante partie de la sécurité de l'ASFC.
- signaler toute attaque ou tentative d'attaque d'ingénierie sociale (connue, soupçonnée ou autrement) à l'égard de la gestion ou de la sécurité.

## RÉFÉRENCES


- Wikipédia – Ingénierie sociale (sécurité de l'information)
  http://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information)






Operational Security Standard: Management of Information Technology Security (MITS)

**16.4.11 Software Integrity and Security Configuration**

Safeguards to prevent and detect the integrity of software can help to avoid many potential security incidents.

Departments should configure their operating systems and application software in accordance with security best practices. Departments must configure their systems to control the use of mobile code (e.g. Javascript).

Departments must implement safeguards to "harden" software that is exposed to the Internet (e.g. Web servers and their software) or servers supporting sensitive applications. At a minimum, departments should remove or disable unnecessary services and applications and properly configure user authentication.

Departments should prohibit the use of unauthorized software, and should have a capability to scan networks to detect unauthorized software.

For more information on software hardening and configuration best practices, refer to the best practices issued by the Communications Security Establishment, the National Institute for Standards and Technology, and the Center for Internet Security.






# Directive on Communications Security (COMSEC)

PROTECTION • SERVICE • INTEGRITY





**Table of Contents**















**List of Tables**



This directive takes effect on February 4, 2015.

## 1 Introduction

### 1.1 Purpose
This directive provides the minimum security requirements for the control of accountable Communications Security (COMSEC) material in the Government of Canada (GC).

### 1.2 Authority
This directive is promulgated pursuant to the *Policy on Government Security* (PGS), which delegates Communications Security Establishment Canada (CSEC) as the lead security agency and national authority for the development, approval and promulgation of COMSEC policy instruments and for the development of guidelines and tools related to Information Technology (IT) Security.

### 1.3 Scope
The methods for the control of COMSEC material vary and are determined by the nature of the material itself. The scope of this directive includes:
- COMSEC material, which requires control and accountability within the National COMSEC Material Control System (NCMCS); and

- COMSEC material (other than above), which requires control and local tracking by the COMSEC Custodian through a manual or electronic tracking system outside of the NCMCS.

### 1.4 Definitions

Specific definitions drawn from authoritative sources are included in the **Glossary of Security Terminology.**

### 1.5 Compliance
All GC departments must comply with the baseline security requirements of the *Directives for the Application of Communications Security in the Government of Canada* (ITSD-01A) and this directive. While compliance with these minimum security requirements is the responsibility of each GC department, this does not preclude individual departments from applying more stringent security measures. Departmental directives that exceed the minimum security requirements of Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03) take precedence within that department.

### 1.6 Expected Results
This directive describes courses of action which CSEC has determined are required to achieve a minimum level of control, safeguard and accounting for COMSEC material in departmental communications operations.







## 1.7 Consequence

Failure to comply with this directive may result in escalated administrative controls being placed on a COMSEC Account. In extreme circumstances, a COMSEC Account will be suspended until an external audit is conducted and the Departmental Security Officer (DSO) or DSO-delegated Departmental COMSEC Authority (DCA) has rectified any shortcomings.

## 1.8 Points of Contact

The CBSA points of contact for topics covered by this directive are listed in Table 1 below.

**Table 1 – Contact Information**

| Office | Phone Number | E-mail Address |
|---|---|---|
| COMSEC Program / COMSEC Custodian | 613 952-6041 | CBSA-ASFC_IISD_COMSEC-DISI_SECCOM IISD_COMSEC-DISI_SECCOM@cbsa-asfc.gc.ca |
| Departmental COMSEC Authority (DCA) | 343-291-7757 | Director Infrastructure & Information Security Division |

## 2 National COMSEC Material Control System

## 2.1 Structure and Organization Overview

The NCMCS is a CSEC-approved logistics system which includes the personnel and procedures that enable GC departments to effectively handle and control COMSEC material. The NCMCS provides for the control of COMSEC material through:

- National Central Office of Record (NCOR);
- CBSA COMSEC Accounts; and
- Local Elements.

## 2.2 COMSEC Accounts

GC departments must establish a COMSEC Account before receiving COMSEC material. Normally, only one COMSEC Account is established at each GC department.

The minimum COMSEC Account personnel requirements include:

- A DCA
- A COMSEC Custodian, and
- At least one Alternate COMSEC Custodian.

## 2.3 Local Elements

Local Elements are individuals who are authorized to hold and use COMSEC material. Local Elements are authorized to exchange COMSEC material only with the COMSEC Account. Local Elements are not authorized to re-loan COMSEC material to other Local Elements except through their own COMSEC Account Custodian.







## 3 Personnel

### 3.1 Roles and Responsibilities
All COMSEC Account personnel and other personnel requiring access to COMSEC material must be Canadian citizens.

### 3.2 Departmental Security Officer
The DSO is appointed by CBSA President. Among other duties, as listed in the PGS, the DSO is responsible to manage the departmental security program. For more detail on the roles and responsibilities of the DSO, consult the *Directive on Department Security Management* (DDSM).

### 3.3 Departmental COMSEC Authority
A DCA may be appointed by the DSO to act in his/her stead to manage the departmental COMSEC program. The DCA is responsible for developing, implementing, maintaining, coordinating and monitoring a departmental COMSEC program that is consistent with the PGS and its operational standards. Additionally, the DCA is responsible for the overall control of COMSEC material that has been charged to the departmental COMSEC Account.

### 3.4 COMSEC Custodian
COMSEC Custodians are responsible for the generation, receipt, custody, distribution, disposition or destruction, and accounting of COMSEC material entrusted to their COMSEC Account in accordance with this directive. COMSEC Custodians are also responsible for providing their departmental users with COMSEC equipment troubleshooting support and guidance on the use of key material.

### 3.5 Alternate COMSEC Custodian
The Alternate COMSEC Custodian assists the COMSEC Custodian in the day-to-day activities of the COMSEC Account and performs the duties of the COMSEC Custodian in the temporary absence of the COMSEC Custodian.

### 3.6 Local Element
A Local Element is an individual who is authorized to hold and use COMSEC material. A Local Element is personally responsible for the control, and safeguarding of COMSEC material entrusted to he or she, in accordance with the control and handling instructions provided by their COMSEC Account.

### 3.7 Other Authorized Users
In certain instances, individuals, such as, shift workers and technicians may require short term (immediate) access to COMSEC material. Before allowing this access, the individual who is personally responsible for the COMSEC material must confirm with the COMSEC Custodian or Alternate Custodian that the user requiring access:

- is a Canadian citizen;
- has a need-to-know, has been COMSEC briefed and possesses the required security clearance at the level equal to or higher than the material and information they will access;
- signs for and maintains constant personal surveillance of the COMSEC material until it is returned;
- does not transport the COMSEC material to another work area or building without consent; and







• understands what constitutes a COMSEC incident or potential COMSEC incident (Incident reporting Section 14).

**4 Management of COMSEC Records**

**4.1 Retention/Disposition of Records and Files**
All inactive or archived COMSEC Account records and files must be retained by the Custodian for a period of no less than five years.

**4.2 Classification of Records and Files**
COMSEC Account records and files must be marked "PROTECTED A" unless they contain classified information, in which case it must be marked in accordance with the sensitivity of the content.

**4.3 Access to Records and Files**
The COMSEC Custodian must limit access to COMSEC Account records and files to individuals who have a need-to-know and possess the appropriate security clearance.

**4.4 Changes to COMSEC Accounts**

**4.5 Change of Personnel**
The COMSEC Custodian or Alternate COMSEC Custodian must be informed of any changes of the personnel having access to COMSEC accounting material.

**4.6 Absence of Local Element**

**4.7 Temporary Absence**
In the absence of the Local Element for a period of 60 calendar days or less, the primary Local Element must ensure an Alternate person assumes the responsibilities and duties of the primary Local Element.

**4.8 Absence Longer than 60 Calendar Days**
An absence of more than 60 calendar days must be treated as a permanent absence, and the Local Element must contact the COMSEC Custodian or Alternate COMSEC Custodian to have his/her responsibility transfer to another individual.

**5 Types of COMSEC Material**

**5.1 Key Material**
The term key material applies to both physical and electronic formats of key.

**5.2 COMSEC Equipment**
COMSEC equipment is normally identified and accounted for by one short or long title.

**6 Accounting Forms, Reports and Notices**

**6.1 COMSEC Material Report**







The primary accounting form used for the control of COMSEC material is the multipurpose *COMSEC Material Report* (commonly referred to as the GC-223 form). This form is used to:

- report the change in the status of COMSEC material (e.g. transfer, issue, or destruction);
- report the inventory holdings of a COMSEC Account (i.e. Inventory Report);

**6.1.1 Transfer Report**

The distribution of COMSEC material between two entities is called a transfer. COMSEC material being transferred must be prepared and receipted. The COMSEC Custodian is responsible to draft the Transfer Report.

**6.1.2 Hand Receipt**

The distribution of COMSEC material to a Local Element is called an issue. COMSEC material being issued may be packaged as a shipment or it may be hand delivered directly to an authorized recipient. Packages wrapped for shipment must be prepared in accordance with the direction in Section 10.

**6.1.3 Distribution**

The issuance of COMSEC material is recorded on a Hand Receipt. When distributing COMSEC material to a COMSEC Local Element, the COMSEC Custodian must use a Hand Receipt.

Recipients must sign the Hand Receipt to certify their acceptance of the listed material, as well as an understanding of the handling requirements for the COMSEC material entrusted to them.
Before signing the Hand Receipt, the recipient must inspect the COMSEC material to verify the accuracy of the document and to establish the condition of the material. See Section 10.

**NOTE:** Hand Receipts for COMSEC material must be reviewed annually by the COMSEC Custodian to ensure their accuracy and to verify the continued requirement for Accountable COMSEC Material (ACM) by authorized end-users.

**6.1.4 Accountability**

Accountability for issued COMSEC material includes the CBSA COMSEC Account, and the person assigned as the Local Element. Upon signing the Hand Receipt, the recipient assumes responsibility for the care and control of all material listed on the document; however, the recipient's signature on a Hand Receipt does not relieve the CBSA COMSEC Custodian from accountability for the issued material.

**6.1.5 Confirmation before Issue**

Before issuing COMSEC material to a Local Element, the COMSEC Custodian must ensure the recipient:

- has the need-to-know for COMSEC material listed on the Hand Receipt;
- is a Canadian citizen;
- is cleared to the security level of the COMSEC material listed on the Hand Receipt;
- has been COMSEC briefed and has signed a *COMSEC Briefing Certificate and a Local Element Responsibility*;
- has the appropriate storage facilities for the material listed on the Hand Receipt;
- has been trained on the handling, storage, and use of the COMSEC material listed on the Hand Receipt;







- is aware of what constitutes a COMSEC incident (Incident reporting see section 14). ;
- where necessary, has established a local accounting system that maintains strict control of each item of the COMSEC material listed on the Hand Receipt whenever it must be accounted for during shift work operations; and,
- signs the Hand Receipt acknowledging the receipt of the material and understanding of the responsibilities associated with handling the COMSEC material listed on the Hand Receipt.

**6.1.6 Returning COMSEC Material**

COMSEC Local Elements must return COMSEC material to the COMSEC Custodian if it is no longer required.

COMSEC material issued to a Local Element must be returned to the COMSEC Account that issued the material. The COMSEC Custodian must prepare a Hand Receipt for material being returned from the Local Element. The COMSEC Custodian must ensure that the Hand Receipt, which lists the material being returned from the Local Element, is addressed to the COMSEC Account. The COMSEC Custodian's signature on the Hand Receipt relieves the Local Element from accountability for the returned COMSEC material. Local Elements are not authorized to re-loan COMSEC material to any other Local Elements.

**6.2 Inventory Report**

The COMSEC Custodian is responsible to produce and reconcile a yearly inventory report. During the inventory process, the COMSEC material held at the COMSEC Account is physically sighted and the actual holdings are compared to the accounting records. The inventory process is very important as it is sometimes the only means of discovering the loss of COMSEC material.

**6.3 Accounting Notices**

**6.3.1 Tracer Notice – Transfers**

If the signed COMSEC Material Report (hand receipt) has not been received within 7 business days, tracer action must be initiated as follows:

- The initial tracer action may be accomplished via a documented phone call, e-mail.
- Failure to respond to the Tracer Notices action could result in an immediate verification of the Local Element holdings.

**7 Access to COMSEC Material**

**7.1 Prerequisite for Access to COMSEC Material**

**7.1.1 Access by Government of Canada Employees and Contractors**

Access to COMSEC material may be granted to Canadian citizens who:

- possess a valid GC security clearance commensurate with the security classification of the material and information they will access;
- have a "need-to-know";
- have been given a COMSEC Briefing;







- have signed a COMSEC Briefing Certificate;
- are familiar with applicable COMSEC material control procedures.

**7.1.2 Access by Foreign Nationals**

Access to COMSEC material may be granted to foreign nationals (i.e. non-Canadian citizens) upon approval from CSEC on a case-by-case basis. Requests for such access must be submitted in writing to COMSEC Client Services at CSEC.

**8 COMSEC Briefing and COMSEC Briefing Certificate**

**8.1 Requirements**

The DCA and COMSEC Custodian must ensure individuals requiring access to COMSEC material receive a *COMSEC Briefing* and sign a *COMSEC Briefing Certificate*.

**8.2 Retention of COMSEC Briefing Certificates**

A *COMSEC Briefing Certificate* must be retained by the COMSEC Custodian for a minimum of two years after an individual's authorization to access COMSEC material has ended.

**9 Physical Security**

**9.1 Requirement**

A COMSEC facility must be established wherever COMSEC material is stored, used or operations warrant the maximum possible protection from theft, compromise, damage and deterioration of COMSEC material and ensure access and accounting integrity is maintained.

**10 Distributing COMSEC Material**

When preparing COMSEC material for distribution, the COMSEC Custodian must:

- verify the receiving Local Element is authorized to hold the COMSEC material;
- verify the security classification of the receiving Local Element to ensure they possess the required security clearance at the level equal to or higher than the material and information they will access;
- package components which, as a whole, comprise a cryptographic system separately and transport in different shipments (section 10.2);
- ensure that electronic key material is transmitted in accordance with the applicable system or equipment doctrine (doctrine will be provided in accordance with the type of material in inventory); and
- prepare a COMSEC Material Report in accordance with section 6 of this directive.

**10.1 Tracking the Shipment of COMSEC Material**

Following the shipment of COMSEC material, the COMSEC Custodian must:

- notify the recipient of the details of the shipment and the estimated time of delivery;







- follow-up to ensure the COMSEC material has been delivered to the authorized recipient according to schedule; and
- if a shipment is not received in accordance with the shipment details, initiate shipment tracer action with the carrier to determine the last known location of the shipment.

**10.2 Packaging Physical COMSEC Material**

**10.2.1 Overview**
Packaging used for the distribution of physical COMSEC material will depend upon the material's size, weight, shape and intended method of transport. All COMSEC material must be double-wrapped or otherwise encased in two opaque containers, and securely sealed (including seams) before its transportation.

**10.2.2 Inner Wrapping**
The inner wrapping for package(s) must be secure enough to detect tampering, guard against damage and be marked as follows:

- full addresses of both the shipping and receiving COMSEC Accounts or Local Element address.
- notation "TO BE OPENED ONLY BY" must be noted beside the name of the receiving address.

**10.2.3 Outer Wrapping**
The outer wrapping must:

- be secure enough to prevent damage to the contents or inadvertent or accidental unwrapping;
- not bear any indication that the package contains classified or protected COMSEC material;
- be marked with the:
  - full addresses of both the shipping COMSEC Account and the receiving COMSEC Account or Local Element address, and
  - shipment label or authorized courier label.

**10.2.4 Parcels**
Good quality brown wrapping paper and good quality packing tape should be used when preparing COMSEC parcels. Such parcels must be packaged and bound as follows:

- All seams of the inner wrapping must be bound with a quality clear shipping/packing tape heavy enough to ensure the seams are closed at all the edges.
- Protection of the COMSEC material inside the parcel is to be done by using paper and bubble wrap to prevent possible crushing of the parcel while in transit.
- Outer wrapping must consist of paper and quality clear shipping/packing tape heavy enough to ensure a suitably sturdy parcel.

**10.3 Receiving COMSEC Material**

**10.3.1 Inspection of Packages**
On receipt of a shipment, the COMSEC Custodian or Local Element must:





- carefully inspect the outer wrapping and inner wrapping of the shipment for signs of damage or tampering before removing each wrapping;
- check the addresses on both outer and inner wrapping to confirm the shipment has been sent to the intended recipient;
- immediately report to COMSEC Custodian any evidence of possible tampering with either the inner or outer wrappings or unauthorized access to the contents as a possible COMSEC incident.

**10.3.2 Validation of Content**

When satisfied that the packaging has not been tampered with, the COMSEC Custodian or the Local Element must:

- open the package;
- unpack the contents and confirm that the items listed on the enclosed COMSEC Material Report;
- match the items shipped by confirming the short title, edition and quantities of all items, and accounting numbers, where applicable; and
- report any discrepancies to the shipping COMSEC Custodian.

**11 Tracking**

**11.1 Local Tracking System**

Certain material (e.g. CIKs, PINs) associated with COMSEC equipment, must be controlled by the COMSEC Custodian through a local tracking and control system. It is the responsibility of the originating authority to identify this material. Control and handling of this material will be according to this directive, unless otherwise specified by the applicable equipment doctrine or the originator.

**11.2 Storage of Personal Identification Numbers and Passwords**

When records or lists of PINs or passwords need to be maintained, they must be safeguarded and managed by an appropriate Local Element with guidance from the COMSEC Custodian for protection of the record at the same classification level of the COMSEC material being protected by the PIN or password.

**12 Emergency Destruction**

**12.1 COMSEC Equipment**

In deteriorating conditions, all reasonable efforts must be made to evacuate COMSEC equipment. During an actual emergency, when evacuation may not be possible, the immediate goal is to render COMSEC equipment unusable and irreparable. Consequently, when there is warning of hostile intent, consideration must be given to discontinue secure communications to allow for the thorough destruction of COMSEC equipment. Emergency destruction priorities for COMSEC equipment by zeroization of equipment, if the keying element (e.g. key card, permuter plug) cannot be physically withdrawn.

The three options for the control of COMSEC material in an emergency due to hostile activity are:

- securing COMSEC material;
- removing COMSEC material from the scene of the emergency; and



- destroying COMSEC material.

**12.1 Reporting Emergency Destruction**

Accurate and timely reporting of emergency destruction is essential in order to evaluate the severity of an emergency, and is second in importance only to ensuring that the COMSEC material is thoroughly destroyed. A report must be submitted to COMSEC Custodian as soon as possible. The report must clearly indicate, for the destroyed COMSEC material, the method(s) of destruction, and the degree of destruction. This report must also identify any items that were not destroyed and which may be presumed compromised.

## 13 COMSEC Account Audit

**13.1 Delegation of Authority**

The PGS mandates that CSEC report to the Treasury Board Secretariat (TBS) on the state of COMSEC in the GC when requested. Compliance with this mandate requires CSEC to audit COMSEC Accounts on a regular basis.

**13.2 Purpose of an Audit**

The audit provides an independent review of a COMSEC holding records and activities to ensure COMSEC material produced by or entrusted to the COMSEC Account is controlled as detailed in this directive.

**13.3 Scope of the Audit**

The audit must be sufficient in scope to determine the accuracy of COMSEC accounting records and to confirm that COMSEC material control procedures have been, and continue to be, correctly applied.

**13.4 COMSEC Verification**

**13.4.1 SCOPE**

A CBSA COMSEC Verification is to be conducted by the Regional or HQ Security Manager or their representative to determine the accuracy of COMSEC accounting records and to confirm that COMSEC material control procedures have been, and continue to be, correctly applied. The COMSEC Verification includes:

- verification that COMSEC Material Transfer Reports (Hand Receipt) and files are complete and accurate;
- the physical sighting of accountable COMSEC material;
- COMSEC Verification of all procedures related to the control and safeguarding of COMSEC material; and
- solicitation of problems encountered by the office in maintaining control of the COMSEC material, and the provision of advice.

**13.4.2 COMSEC Verification Check Lists**







**Purpose:** COMSEC Verification check lists are designed to ensure that all aspects of COMSEC management are being appropriately maintained by the CBSA Local Element (i.e. the person responsible for the COMSEC equipment).

**Preparation:** In preparation for a COMSEC Verification, the RSM or their representative is to contact the COMSEC Coordinator to request the latest information of the site to be visited. The COMSEC Coordinator will provide the location, the name of the person responsible for the COMSEC material, the type of equipment with their serial number, the security level involved and the list of the registered user(s).

## 14 COMSEC Incidents

### 14.1 General

A COMSEC incident occurs whenever there is a situation or activity that jeopardizes the confidentiality, integrity or availability of COMSEC information, material or services.
Prompt and accurate reporting of COMSEC incidents minimizes the potential for compromise of COMSEC material and the classified information that it protects. Unless all personnel who handle or manage COMSEC material immediately report all occurrences that are specifically identified as COMSEC incidents, corrective action cannot be implemented in a timely manner to mitigate or eliminate their impact.

It is vitally important that all suspected COMSEC incidents be promptly reported to the COMSEC Custodian. COMSEC incidents are not reported through the Security Incident Reporting process.

### 14.2 Classes of COMSEC Incidents

#### 14.2.1 Compromising Incidents

Compromising incidents may have serious consequences for operational security. Investigation of compromising incidents helps to determine if sensitive records were irretrievably lost by the rightful owners or accessed by an unauthorized individual. It is important to note that the compromise of sensitive information or asset(s) may have implications far beyond the local authorized user or GC department. Compromising incidents are reportable at the national level (report to COMSEC Custodian, DCA and the National COMSEC Incidents Office [NCIO]).

#### 14.2.2 Practices Dangerous to Security

Practices Dangerous to Security (PDS) are incidents that are considered minor violations of administrative requirements and do not result in the loss of control, unauthorized access or unauthorized viewing of COMSEC material. **PDS are considered administrative infractions and are not reportable at the national level**. PDS do not result in a compromise of information, assets or functionality, but create situations where exploitation is possible unless action is taken to correct the practice. Even minor violations may warrant an evaluation.
Therefore, PDS must be handled locally by the DCA in accordance with departmental directives.

#### 14.2.3 Example of COMSEC Incidents

Such incidents include:







- the use of key material which is compromised, superseded, defective, previously used (and not authorized for reuse) or incorrectly used. For example the:
  - unauthorized use of any key material for other than its intended purpose
  - unauthorized extension of a crypto period;, and
  - premature use of key material; and
  - use of COMSEC systems, equipment, software, operational practices or maintenance practices which are not approved by CSEC.
- theft of COMSEC material;
- deliberate falsification of COMSEC records or reports;
- known or deliberate failing to report a known or suspected COMSEC incident;
- unauthorized disclosure, or an attempt at disclosure, of information concerning COMSEC material;
- accidentally or knowingly processing, storing or transmitting classified or protected information on an inappropriate COMSEC system or equipment;
- loss of any COMSEC material or portions thereof;
- unauthorized access to COMSEC material;
- discovery of COMSEC material outside of required accountability and physical control. For example:
  - material left unsecured and unattended where unauthorized individuals could have had access;
  - COMSEC material improperly packaged or shipped;
  - known or suspected tampering with or penetration of COMSEC material including, but not limited to, COMSEC material received in protective packaging which shows evidence of tampering and unauthorized premature opening of a sealed package of key material; and
  - any other occurrence which jeopardizes the physical security of COMSEC material.

**14.2.4 Handling of Incidents**

The COMSEC Custodian must ensure that each individual who uses, or otherwise has access to COMSEC material is capable of recognizing a COMSEC incident and understands the requirements for **immediately** reporting COMSEC incidents.

**14.2.5 Consequences**

The primary purpose of reporting COMSEC incidents is to continuously maintain the maximum possible level of protection for GC sensitive information and COMSEC material. Failure to report a COMSEC incident, or cover it up, may be considered "wilful or gross neglect" and must be evaluated accordingly. The DCA is responsible for investigating and responding to reports of non-compliance with this policy and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies; directives or standards may be subject to disciplinary action, up to and including termination of employment.

In cases of non-compliance, CSEC may escalate administrative control of a department's COMSEC Account including suspension.





Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive sur la sécurité des communications (COMSEC)

PROTECTION • SERVICE • INTÉGRITÉ

Canada



Table des matières



**Liste des tableaux**



Cette directive entre en vigueur le 4 février 2015.

## 1. Introduction

### 1.1 Objet

La présente directive fournit les exigences de sécurité minimales pour le contrôle du matériel comptable de sécurité des communications (COMSEC pour Communications Security) au sein du gouvernement du Canada (GC).

### 1.2 Autorité

La présente directive est diffusée conformément à la *Politique* sur *la sécurité du gouvernement (PSG)* en vertu de laquelle le Centre de la sécurité des télécommunications Canada (CSTC) est le principal organisme responsable de la sécurité et l'autorité nationale pour l'élaboration, l'approbation et la promulgation des instruments de politique liés à la COMSEC et de l'élaboration des lignes directrices et des outils en lien avec la sécurité des technologies d'information (TI).

### 1.3 Portée

Les méthodes de contrôle du matériel COMSEC varient selon la nature de ce matériel. La portée de la présente directive englobe :

- le matériel COMSEC, qui doit être contrôlé et comptabilisé dans le Système national de contrôle du matériel COMSEC (SNCMC);
- le matériel COMSEC (autre que celui indiqué ci-dessus), qui doit faire l'objet d'un contrôle et d'un suivi local par le gardien COMSEC au moyen d'un système de suivi manuel ou électronique autre que le SNCMC.

### 1.4 Définitions

Des définitions précises provenant de sources qui font autorité se trouvent à au **Lexique de la terminologie en sécurité**.

### 1.5 Conformité

Tous les ministères du GC doivent se conformer aux exigences de base en matière de sécurité des *Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada* (ITSD-01A) et de la présente directive. Quoiqu'il incombe à chaque ministère du GC de se conformer à ces exigences minimales en matière de sécurité, rien n'empêche un ministère d'appliquer des mesures de sécurité plus strictes. Les directives ministérielles qui dépassent les exigences minimales en matière de sécurité stipulées dans la Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada (ITSD-03) ont préséance dans ce ministère.

### 1.6 Résultats escomptés

La présente directive décrit les lignes de conduite que le CSTC juge essentielles pour assurer un niveau minimum de contrôle, de protection et de comptabilité pour le matériel COMSEC dans les activités de communications ministérielles.







**1.7 Conséquences**
La non-conformité à la présente directive peut donner lieu à l'application de contrôles administratifs accrus sur un compte COMSEC. Dans des circonstances extrêmes, un compte COMSEC sera suspendu jusqu'à ce qu'une vérification externe soit réalisée et que l'agent de sécurité du ministère (ASM) ou l'autorité COMSEC du ministère (ACM) déléguée par l'ASM ait corrigé les lacunes.

**1.8 Coordonnées**

Les coordonnées des bureaux de l'ASFC pour les sujets couverts dans la présente directive sont données dans le tableau 1 ci-dessous.

**Tableau 1 – Coordonnées**

| Bureau | Numéro de téléphone | Courriel |
|---|---|---|
| Programme COMSEC / Gardien COMSEC | 613 952-6041 | CBSA-ASFC_IISD_COMSEC-DISI_SECCOM IISD_COMSEC-DISI_SECCOM@cbsa-asfc.gc.ca |
| Responsable ministériel de COMSEC | 343-291-7757 | Directeur de la Division de l'infrastructure et de la sécurité de l'information |

**2 Système national de contrôle du matériel COMSEC**
**2.1 Aperçu de la structure et de l'organisation**
Le SNCMC est un système logistique approuvé par le CSTC qui comprend le personnel et les procédures permettant aux ministères du GC de manutentionner et de contrôler efficacement le matériel COMSEC. Le SNCMC assure le contrôle du matériel COMSEC par l'entremise des éléments suivants :

- Bureau national des dossiers (NCOR)
- Comptes COMSEC de l'ASFC
- Éléments locaux

**2.2 Comptes COMSEC**
Un ministère du GC doit établir un compte COMSEC avant de pouvoir recevoir du matériel COMSEC. En règle générale, un ministère du GC n'établit qu'un seul compte COMSEC.

Le personnel du compte COMSEC doit comprendre au minimum
- un ACM,
- un gardien COMSEC,
- au moins un gardien COMSEC suppléant.

**2.3 Éléments locaux**
Les éléments locaux sont des personnes autorisées à détenir et à utiliser du matériel COMSEC. Les éléments locaux sont autorisés à échanger du matériel COMSEC uniquement avec le compte COMSEC.







Les éléments locaux ne sont **pas** autorisés à prêter du matériel COMSEC à d'autres éléments locaux, sauf par l'intermédiaire du gardien de leur compte COMSEC.

**3 Personnel**

**3.1 Rôles et responsabilités**
Tous les membres du personnel du compte COMSEC et le personnel devant accéder à du matériel COMSEC doivent être des citoyens canadiens.

**3.2 Agent de sécurité du ministère**
L'ASM est nommé par le président de l'ASFC. Parmi les tâches énumérées dans la PSG, l'ASM est responsable de la gestion du programme de sécurité du ministère. Pour plus de détails sur les rôles et responsabilités de l'ASM, se reporter à la *Directive sur la gestion de la sécurité ministérielle* (DGSM).

**3.3 Autorité COMSEC du ministère**
L'ASM peut nommer une ACM pour gérer en son nom le programme COMSEC du ministère. L'ACM est responsable de l'élaboration, de la mise en œuvre, de la tenue, de la coordination et du suivi d'un programme COMSEC ministériel qui est conforme à la PSG et à ses normes opérationnelles. De plus, l'ACM est responsable du contrôle général du matériel COMSEC qui a été porté au compte COMSEC du ministère conformément à la présente directive.

**3.4 Gardien COMSEC**
Les gardiens COMSEC sont responsables de la génération, de la réception, de la garde, de la distribution, de la disposition ou de la destruction, et de la comptabilité du matériel COMSEC porté à leur compte COMSEC conformément à la présente directive. Ils sont également chargés d'offrir aux utilisateurs de leur ministère du soutien relativement au dépannage de l'équipement COMSEC et de l'orientation sur l'utilisation du matériel de chiffrement.

**3.5 Gardien COMSEC suppléant**
Le rôle du gardien COMSEC suppléant est d'assister le gardien COMSEC dans ses tâches quotidiennes liées au compte COMSEC et d'exercer les fonctions du gardien COMSEC en l'absence temporaire de ce dernier.

**3.6 Élément local**
Un élément local est une personne autorisée à détenir et à utiliser du matériel COMSEC.
Les éléments locaux sont personnellement responsables du contrôle, de la protection du matériel COMSEC qui leur a été confié, conformément aux instructions en matière de contrôle et de manutention qui leur ont été transmises par leur gardien du compte COMSEC.

**3.7 Autres utilisateurs autorisés**
Dans certains cas, il est possible que des personnes telles des travailleurs de quarts et des techniciens nécessitent un accès à court terme (immédiat) au matériel COMSEC. Avant d'accorder cet accès, la personne qui est personnellement responsable du matériel COMSEC doit confirmer auprès de l'ACM, du gardien COMSEC ou du gardien suppléant que l'utilisateur nécessitant l'accès :

- est citoyen canadien;







- a un besoin de connaître, a suivi une séance d'initiation COMSEC et détient la cote de sécurité équivalente ou supérieure à celle du matériel et de l'information auxquels il aura accès;
- signe un accusé de réception pour le matériel COMSEC et garde celui-ci sous sa surveillance personnelle constante jusqu'à ce qu'il doive le retourner;
- ne transporte pas le matériel COMSEC dans une autre aire de travail ou dans un autre immeuble sans consentement préalable; et
- comprend ce qui constitue un incident COMSEC ou un incident COMSEC potentiel (rapport sur les incidents, section 14).

## 4 Gestion des dossiers COMSEC

### 4.1 Conservation et disposition des documents et dossiers
Le gardien doit conserver tous les documents et dossiers inactifs ou archivés du compte COMSEC pendant une période minimale de cinq ans.

### 4.2 Classification des documents et dossiers
Les documents et dossiers du compte COMSEC doivent porter la mention PROTÉGÉ A, à moins qu'ils ne contiennent des renseignements classifiés, auquel cas ils doivent être marqués en fonction de la sensibilité du contenu.

### 4.3 Accès aux documents et dossiers
Le gardien COMSEC doit limiter l'accès aux documents et dossiers du compte COMSEC aux personnes qui adhèrent au principe du besoin de connaître et qui possèdent l'habilitation de sécurité appropriée.

### 4.4 Changements aux comptes COMSEC

### 4.5 Changements au personnel
Le gardien COMSEC ou son suppléant doit être informé de tout changement relatif aux membres du personnel ayant accès au matériel de comptabilité COMSEC.

### 4.6 Absence d'élément local

### 4.7 Absence temporaire
En l'absence de l'élément local pendant une période de 60 jours civils ou moins, l'élément local doit veiller à ce qu'une autre personne assume les responsabilités et les fonctions de l'élément local.

### 4.8 Absence supérieure à 60 jours civils
Une absence de plus de 60 jours civils doit être traitée comme une absence permanente, et l'élément local doit communiquer avec le gardien COMSEC ou son suppléant pour faire transférer les responsabilités à une autre personne.

## 5 Types de matériel COMSEC







**5.1 Matériel de chiffrement**
Le terme « matériel de chiffrement » s'applique aux formats physique et électronique des clés.

**5.2 Équipement COMSEC**
L'équipement COMSEC est généralement identifié et comptabilisé au moyen de son titre abrégé ou de son titre au long.

**6 Formulaires, rapports et avis comptables**
**6.1 Rapport de matériel COMSEC**
Le formulaire *Rapport de matériel COMSEC* (généralement appelé le GC-223) est le principal formulaire utilisé pour le contrôle du matériel COMSEC. Ce formulaire sert à :

- communiquer tout changement dans l'état du matériel COMSEC (p. ex. transfert, remise ou destruction);
- communiquer de l'information sur les stocks d'un compte COMSEC (p. ex. rapport d'inventaire).

**6.1.1 Rapport de transfert**
La distribution d'un matériel COMSEC entre deux entités s'appelle un « transfert ». Le matériel COMSEC faisant l'objet d'un transfert doit être préparé et réceptionné. Le gardien COMSEC est responsable de la rédaction du rapport de transfert.

**6.1.2 Accusé de réception**
La distribution du matériel COMSEC à un élément local s'appelle une « remise ». Le matériel COMSEC faisant l'objet d'une remise peut être expédié sous forme de colis ou livré en mains propres au destinataire. Les colis emballés aux fins d'expédition doivent être préparés conformément aux dispositions du section10.

**6.1.3 Diffusion**
La remise d'un matériel COMSEC est consignée sur un accusé de réception. Lorsqu'il distribue du matériel COMSEC à un élément local, le gardien COMSEC doit utiliser un accusé de réception.

En signant l'accusé de réception, le destinataire atteste qu'il accepte le matériel listé et qu'il comprend les exigences de manutention du matériel COMSEC qui lui a été confié. Avant de signer l'accusé de réception, le destinataire doit inspecter le matériel COMSEC pour confirmer que celui-ci concorde avec le document et pour en établir la condition.
Avant de signer l'accusé de réception, le destinataire doit inspecter le matériel COMSEC pour confirmer que celui-ci concorde avec le document et pour en établir la condition. Voir la section 10.

NOTA : Le gardien COMSEC doit passer en revue annuellement les accusés de réception pour les matériaux COMSEC afin de confirmer que chaque utilisateur final autorisé détient toujours le matériel qui lui a été remis et qu'il  a toujours besoin du  Matériel COMSEC comptable (MCC).

**6.1.4 Responsabilité**
La responsabilité pour le matériel COMSEC remis repose sur le compte COMSEC de l'ASFC et la personne occupant la fonction d'élément local. Après avoir signé l'accusé de réception, le destinataire assume la responsabilité pour le soin et le contrôle de tout le matériel figurant sur le document; la signature du destinataire sur l'accusé de réception ne relève toutefois pas le gardien COMSEC de l'ASFC de sa responsabilité envers le matériel remis.





**6.1.5 Confirmation avant remise**
Avant de remettre du matériel COMSEC à l'élément local, le gardien COMSEC doit s'assurer que le destinataire :

- adhère au principe du besoin de connaître en ce qui a trait au matériel COMSEC figurant sur l'accusé de réception;
- est citoyen canadien
- possède une cote de sécurité au niveau correspondant au matériel COMSEC figurant sur l'accusé de réception;
- a suivi une séance d'initiation COMSEC et à signer une attestation d'initiation COMSEC ainsi que *le* document sur les responsabilités de l'élément local.
- dispose des installations d'entreposage requises pour le matériel COMSEC figurant sur l'accusé de réception;
- a reçu la formation appropriée concernant la manutention, l'entreposage et l'utilisation du matériel COMSEC figurant sur l'accusé de réception;
- est au courant de ce qui constitue un incident COMSEC (rapport sur les incidents, voir section 14);
- au besoin, a établi un système de comptabilité locale qui lui permet d'exercer un contrôle rigoureux sur chaque article du matériel COMSEC figurant sur l'accusé de réception lorsqu'il doit être comptabilisé durant des opérations de travail par quarts; et
- signe l'accusé de réception pour attester la réception du matériel remis et sa compréhension des responsabilités associées à la manutention du matériel COMSEC figurant sur l'accusé de réception.

**6.1.6 Retour du matériel COMSEC**
Les éléments locaux COMSEC doivent retourner le matériel COMSEC au gardien COMSEC lorsqu'ils n'en ont plus besoin.

Le matériel COMSEC remis à un élément local doit être retourné au compte COMSEC ayant remis le matériel. Le gardien COMSEC doit préparer un accusé de réception pour le matériel retourné par l'élément local. Le gardien COMSEC doit veiller à ce que l'accusé de réception, qui liste le matériel retourné par l'élément local, soit adressé au compte COMSEC. En signant l'accusé de réception, le gardien COMSEC relève l'élément local de sa responsabilité envers le matériel COMSEC retourné. Les éléments locaux ne sont pas autorisés à prêter du matériel COMSEC à d'autres éléments locaux.

**6.2 Rapport d'inventaire**

Le gardien COMSEC est responsable de la préparation et de l'ajustement d'un rapport annuel d'inventaire. Durant le processus d'inventaire, le matériel COMSEC détenu par le compte fait l'objet d'un contrôle à vue et les articles en stock sont comparés aux dossiers comptables. Le processus d'inventaire est très important, car c'est parfois le seul moyen de découvrir la perte d'un matériel COMSEC.

**6.3 Avis comptables**

**6.3.1 Avis de recherche — Transferts**



Si le rapport matériel COMSEC (accusé de réception) n'a pas été reçu dans les 7 jours ouvrables, il faut entreprendre une demande de recherche comme suit :

- La demande de recherche initiale peut être effectuée au moyen d'un appel téléphonique documenté ou d'un courriel.
- L'absence de réponse aux avis de recherche peut entraîner la vérification immédiate de l'inventaire de l'élément local.

**7 Accès au matériel COMSEC**

**7.1 Conditions préalables à l'accès au matériel COMSEC**

**7.1.1 Accès par des employés ou des entrepreneurs du gouvernement du Canada**
L'accès au matériel COMSEC peut être accordé aux citoyens canadiens qui :

- détiennent une cote de sécurité valide du GC correspondant au niveau de classification de sécurité du matériel et de l'information auxquels ils ont accès;
- satisfont au principe du besoin de connaître;
- ont assisté à une séance d'initiation COMSEC;
- ont signé une attestation d'initiation COMSEC;
- connaissent bien les procédures de contrôle du matériel COMSEC applicables.

**7.1.2 Accès par des ressortissants étrangers**
L'accès au matériel COMSEC peut être accordé à des ressortissants étrangers (c.-à-d. des citoyens non canadiens) sur approbation du CSTC, au cas par cas. Les demandes à cet égard doivent être soumises par écrit aux Services à la clientèle en matière de COMSEC, au CSTC.

**8 Séances d'initiation COMSEC et attestations d'initiation COMSEC**

**8.1 Exigences**
L'ACM et le gardien COMSEC doivent veiller à ce que toute personne nécessitant l'accès à du matériel COMSEC assiste à une *séance d'initiation COMSEC* et signe une *attestation d'initiation COMSEC*.

**8.2 Conservation des attestations d'initiation COMSEC**
Le gardien COMSEC doit conserver *l'attestation d'initiation COMSEC* d'une personne pendant une période minimale de deux ans après que son autorisation d'accès au matériel COMSEC a pris fin.

**9 Sécurité physique**

**9.1 Exigences**

Il faut établir une installation COMSEC là où l'on entrepose ou utilise du matériel COMSEC ou là où les activités justifient une protection maximale contre le vol, l'altération, les dommages et la détérioration du matériel COMSEC, et veiller à ce que l'intégrité de l'accès et des responsabilités soit maintenue.

**10 Distribution du matériel COMSEC**
Lorsqu'il prépare le matériel COMSEC aux fins de distribution, le gardien COMSEC doit :







- s'assurer que l'élément local destinataire est autorisé à détenir le matériel COMSEC;
- vérifier la cote de sécurité de l'élément local destinataire pour veiller à ce qu'il détienne la cote de sécurité de niveau équivalent ou supérieur à la classification du matériel et de l'information auxquels il aura accès;
- emballer séparément les composants qui, ensemble, constituent un système cryptographique et les expédier dans des envois différents (voir section 10.2);
- veiller à ce que le matériel de chiffrement électronique soit transmis conformément à la doctrine du système ou de l'équipement connexe (la doctrine sera fournie selon le type de matériel en réserve);
- préparer un rapport de matériel COMSEC conformément à la section 6 de la présente directive.

**10.1 Suivi des envois de matériel COMSEC**

Après l'envoi de matériel COMSEC, le gardien COMSEC doit :

- aviser le destinataire des détails de l'envoi et de l'heure approximative de livraison;
- faire le suivi de l'envoi afin de s'assurer que le matériel COMSEC a été livré au destinataire autorisé dans les délais prescrits;
- si un envoi n'a pas été reçu selon les renseignements de livraison, lancer une mesure de suivi auprès du transporteur pour déterminer le dernier emplacement connu de l'envoi.

**10.2 Emballage du matériel COMSEC physique**

**10.2.1 Aperçu**

L'emballage utilisé pour la distribution du matériel COMSEC physique dépendra de la taille, du poids et de la forme de ce dernier, de même que du moyen de transport utilisé. Tout le matériel COMSEC doit être expédié sous double emballage, ou encore déposé dans deux contenants opaques, et soigneusement cacheté (y compris les joints) avant son transport.

**10.2.2 Emballage intérieur**

L'emballage intérieur doit être suffisamment sécurisé pour permettre de détecter tout trafiquage et de protéger le matériel contre l'endommagement, il et doit porter les mentions suivantes :

- l'adresse complète des comptes COMSEC expéditeur et destinataire ou l'adresse de l'élément local;
- l'inscription « NE PEUT ÊTRE OUVERT QUE PAR » doit être indiquée à côté du nom du destinataire.

**10.2.3 Emballage extérieur**

L'emballage extérieur :

- doit être suffisamment sécurisé pour empêcher tout endommagement au contenu ou tout déballage accidentel ou par inadvertance;
- ne doit porter aucune indication que le colis contient du matériel COMSEC classifié ou protégé;
- doit porter les mentions suivantes :
  - l'adresse complète des comptes COMSEC expéditeur et destinataire, ou l'adresse de l'élément local;
  - l'étiquette d'envoi ou du messager autorisé.







### 10.2.4 Colis

Les colis contenant du matériel COMSEC doivent être emballés dans du papier brun de bonne qualité et cachetés à l'aide d'un ruban de bonne qualité. De tels colis doivent être confectionnés et attachés comme suit :

- Tous les joints de l'emballage intérieur doivent être maintenus par un ruban adhésif transparent de bonne qualité pour veiller à ce que toutes les intersections soient fermées.
- Du papier et un film à bulles servent à protéger le matériel COMSEC dans le colis afin d'éviter que le contenu ne soit écrasé au cours du transport.
- L'emballage extérieur doit être constitué de papier et de ruban transparent suffisamment épais pour former un colis solide.

## 10.3 Réception du matériel COMSEC

### 10.3.1 Inspection des colis

À la réception d'un envoi, le gardien COMSEC ou l'élément local doit procéder comme suit :

- examiner attentivement les emballages extérieurs et intérieur du colis pour relever tout signe de dommage ou de trafiquage possible avant de retirer chaque emballage;
- vérifier les adresses sur les emballages extérieur et intérieur pour confirmer que le colis a bel et bien été livré au bon destinataire;
- communiquer sur-le-champ au gardien COMSEC tout signe de trafiquage de l'emballage intérieur ou extérieur ou encore l'accès non autorisé au contenu comme incident COMSEC possible.

### 10.3.2 Validation du contenu

Lorsqu'il est convaincu qu'il n'y a pas eu trafiquage du colis, le gardien COMSEC ou l'élément local doit :

- ouvrir le colis;
- déballer le contenu et vérifier si les articles figurant sur le rapport de matériel COMSEC;
- correspondent aux articles expédiés en confirmant;
- le titre abrégé, l'édition et la quantité de tous les articles, les numéros de comptabilité, au besoin; et
- signaler tout écart au gardien COMSEC expéditeur.

# 11 Suivi

## 11.1 Système de suivi local

Le gardien COMSEC doit contrôler au moyen d'un système de contrôle et de suivi local tout matériel (p. ex. CIK, NIP) qui est associé à l'équipement COMSEC. La responsabilité d'identifier ce matériel relève de l'autorité d'origine. Le contrôle et la manutention de ce matériel doivent se conformer à la présente directive, sauf indication contraire dans la doctrine de l'équipement connexe ou par l'autorité d'origine.

## 11.2 Rangement des numéros d'identification personnels et des mots de passe

Lorsqu'ils doivent être conservés, les dossiers ou de listes de NIP ou de mot de passe, doivent être protégés et gérés par l'élément local selon les directives du gardien COMSEC pour la protection des dossiers ayant le même degré de classification que le matériel COMSEC protégé par le NIP ou le mot de passe.







## 12 Destruction d'urgence

### 12.1 Équipement COMSEC

Lorsque les conditions se détériorent, il faut déployer tous les efforts raisonnables pour évacuer l'équipement COMSEC. Dans le cadre d'une urgence réelle, lorsqu'une évacuation n'est pas possible, le but immédiat est de rendre l'équipement COMSEC inutilisable et irréparable. Par conséquent, à la réception d'un avertissement d'intention hostile, il faut envisager d'interrompre les communications sécurisées afin de permettre la destruction totale de l'équipement COMSEC. Si l'élément de mise à la clé (p. ex. carte-clé, fiche de permutation) ne peut physiquement être retiré, pour procéder à la destruction d'urgence de l'équipement COMSEC, il faut faire la mise à zéro de l'équipement.

Les trois options liées au contrôle du matériel COMSEC dans une situation d'urgence résultant d'activités hostiles sont les suivantes :

- mettre le matériel COMSEC en lieu sûr;
- retirer le matériel COMSEC des lieux de l'urgence; et
- détruire le matériel COMSEC.

### 12.1 Rapport de destruction d'urgence

Il est essentiel de préparer un rapport exact et opportun de la destruction d'urgence afin d'évaluer la gravité de l'urgence, la seule chose plus importante étant de veiller à ce que le matériel COMSEC soit entièrement détruite. Le rapport doit être soumis au gardien COMSEC dans les plus brefs délais. Il doit indiquer clairement, pour le matériel COMSEC détruit, la ou les méthodes de destruction et le degré de la destruction. Ce rapport doit également énumérer tous les articles qui n'ont pas été détruits et qui peuvent être présumés compromis.

## 13 Vérification des comptes COMSEC

### 13.1 Délégation des pouvoirs

En vertu de la PSG, le CSTC doit faire rapport au Secrétariat du Conseil du Trésor (SCT) sur l'état de la COMSEC au GC, sur demande. Pour se conformer aux exigences de cette politique, le CSTC doit effectuer la vérification des comptes COMSEC de façon régulière.

### 13.2 Objet de la vérification

La vérification offre un processus d'examen indépendant des dossiers des avoirs et activités COMSEC dans le but d'assurer que le matériel COMSEC produit par le compte, ou confié à celui-ci, est contrôlé comme il est décrit en détail dans la présente directive.

### 13.3 Réalisation de la vérification

La portée de la vérification d'un compte COMSEC devrait permettre de déterminer si les enregistrements COMSEC comptables sont exacts et si les procédures de contrôle du matériel ont été suivies correctement et continuent de l'être.

### 13.4 Vérification de COMSEC

#### 13.4.1 PORTÉE







Une vérification COMSEC de l'ASFC doit être effectuée par le gestionnaire régional de la sécurité (ou de l'Administration centrale) ou son représentant afin de déterminer si les enregistrements COMSEC comptables sont exacts et si les procédures de contrôle du matériel ont été suivies correctement et continuent de l'être. La vérification comprends :

- la vérification que les rapports de transfert de matériel de COMSEC (accusés réception) et que les dossiers sont complets et exacts;
- le contrôle à vue du matériel COMSEC comptable;
- La vérification COMSEC de toutes les procédures liées au contrôle et à la protection du matériel COMSEC; et
- des questions sur les problèmes encourus par le bureau lors du contrôle du matériel COMSEC, ainsi que des conseils à ce sujet.

**13.4.2 Liste de vérification de COMSEC**

**Objet** : Les listes de vérification COMSEC sont conçues pour veiller à ce que l'élément local de l'ASFC (la personne responsable du matériel COMSEC) se conforme à tous les aspects de la gestion COMSEC de façon appropriée.

**Préparation :** Pour se préparer à la vérification COMSEC, le GRS ou son représentant doit communiquer avec le coordinateur COMSEC pour demander les renseignements les plus récents au sujet du lieu à visiter. Le coordonnateur COMSEC fournira le lieu, le nom du responsable du matériel COMSEC, le type d'équipement et leurs numéros de série, le niveau de sécurité et la liste des utilisateurs enregistrés.

**14 Incidents COMSEC**

**14.1 Généralités**

Un incident COMSEC se produit chaque fois qu'une situation ou activité compromet la confidentialité, l'intégrité ou la disponibilité de l'information, du matériel ou des services COMSEC.
Le signalement rapide et exact des incidents COMSEC permet de réduire au minimum la possibilité de compromission d'un matériel COMSEC et de l'information classifiée qu'il protège. À moins que les membres du personnel qui manutentionnent ou gèrent du matériel COMSEC ne signalent immédiatement toutes les occurrences d'incidents définis spécifiquement comme étant des incidents COMSEC, il est impossible de mettre en œuvre de façon opportune des mesures correctives pour en atténuer ou en éliminer les répercussions.

Il est d'une suprême importance que chaque incident COMSEC présumé soit signalé au gardien COMSEC dans les plus brefs délais. Les incidents COMSEC ne sont pas indiquées au moyen du processus de déclaration des incidents de sécurité.

**14.2 Classes d'incidents COMSEC**

**14.2.1 Incidents compromettants**

Les incidents compromettants peuvent porter un grave préjudice à la sécurité opérationnelle. L'enquête sur les incidents compromettants sert à déterminer si des enregistrements sensibles ont été irrémédiablement perdus par leurs propriétaires légitimes ou si une personne non autorisée y a accédé. Il est important de noter que la compromission de biens ou de renseignements sensibles peut avoir des







répercussions bien au-delà de l'utilisateur local autorisé ou du ministère. Les incidents compromettants doivent être signalés au niveau national (au gardien COMSEC, à l'AMC et au le Bureau national des incidents COMSEC (BNIC)).

**14.2.2 Pratiques dangereuses pour la sécurité**

Les pratiques dangereuses pour la sécurité (PDS) sont des incidents considérés comme des infractions mineures à des exigences administratives, qui ne donnent pas lieu à la perte de contrôle, à l'accès non autorisé ou à l'exposition non autorisée de matériel COMSEC. **Les PDS sont considérées comme des infractions administratives et ne sont pas signalées à l'échelle nationale**. Elles ne débouchent pas nécessairement sur une compromission de l'information, d'un bien ou d'une fonctionnalité, mais créent des situations pouvant donner lieu à une exploitation à moins que des mesures ne soient prises pour corriger la pratique. Même les infractions mineures peuvent justifier une évaluation.
Par conséquent, les PDS doivent être traitées localement par l'ACM conformément aux directives ministérielles.

**14.2.3 Exemples d'incidents COMSEC**

Ces incidents comprennent notamment :

- emploi d'un matériel de chiffrement compromis, remplacé, défectueux, déjà utilisé (dont la réutilisation n'a pas été autorisée) ou mal utilisé. Par exemple :
    - emploi non autorisé du matériel de chiffrement à une autre fin que son utilisation prévue
    - prolongement non autorisé d'une période cryptographique
    - utilisation prématurée d'un matériel de chiffrement;
    - emploi de systèmes, d'un équipement, de logiciels, de pratiques opérationnelles ou de pratiques de maintenance COMSEC qui ne sont pas approuvés par le CSTC.
- vol de matériel COMSEC;
- falsification délibérée des registres ou rapports COMSEC;
- omission connue ou délibérée de signaler un incident COMSEC connu ou soupçonné;
- divulgation ou tentative de divulgation non autorisée d'une information relative au matériel COMSEC;
- traitement, entreposage ou transmission accidentels ou délibérés d'une information classifiée ou protégée sur un système ou un équipement COMSEC non adéquat;
- perte de matériel COMSEC en totalité ou en partie;
- accès non autorisé au matériel COMSEC;
- découverte d'un matériel COMSEC échappant aux contrôles comptables ou physiques requis. Par exemple :
    - matériel non sécurisé laissé sans surveillance à un endroit auquel des personnes non autorisées pouvaient avoir accès,
    - emballage ou envoi inadéquat de matériel COMSEC; et
    - trafiquage ou pénétration connus ou soupçonnés d'un matériel COMSEC, y compris, mais sans s'y limiter, le matériel COMSEC reçu dans un conditionnement protecteur montrant des signes de trafiquage et d'ouverture prématurée d'un paquet scellé de matériel de chiffrement;
    - tout autre incident mettant en péril la sécurité physique du matériel COMSEC.

**14.2.4 Traitement des incidents**





Le gardien COMSEC doit faire en sorte que chaque personne qui utilise du matériel COMSEC, ou qui y a accès, soit en mesure de reconnaître un incident COMSEC et comprenne les exigences liées à leur signalement **immédiat**.

### 14.2.5 Conséquences

Le signalement des incidents COMSEC vise avant tout à assurer un niveau maximal de protection de l'information sensible et du matériel COMSEC du GC. Le fait d'omettre de signaler un incident COMSEC, ou de le dissimuler, est considéré comme « une négligence volontaire ou grossière » et doit être évaluée en conséquence. L'ACM est responsable des enquêtes et des réponses aux rapports de non-conformité à la politique, et doit veiller à ce que les mesures de correction appropriées soient prises au besoin. Tout employé qui enfreint des politiques, des directives ou des normes peut faire l'objet de mesures disciplinaires pouvant aller jusqu'au licenciement.

Dans les cas de non-conformité, le CSTC peut appliquer un contrôle administratif plus rigoureux au compte COMSEC ministériel en cause pouvant aller jusqu'à la suspension.


Canada Border Services Agency | Agence des services frontaliers du Canada




The information you provide in this document is collected under the authority of ***Section 7(1)*** of the ***Financial Administration Act*** and the ***Government of Canada's Policy on Government Security (PGS)*** for the purposes of employee security screening. The information collected may be disclosed to the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), and to entities outside the federal government (e.g. credit bureaus) for the purposes of employee security screening.

Individuals have the right of access to, the protection and correction of their personal information under the ***Privacy Act - Section 12***. The information collected is described under the Personnel Security Screening Program CBSA PPU 1108 Personal Information Bank which is detailed at www.infosource.gc.ca.

## Justification for Initial or Update Indoctrinations to Special Intelligence (SI) Access

In accordance with the Canadian SIGINT Security Standards, Communications Security Establishment Canada, anyone who requires direct access to SI and Si-related information must:

- Be sponsored by an authority in the department requesting direct access to Special Intelligence on behalf of an individual;
- Be a Canadian Citizen;
- Hold a Top Secret security clearance;
- Provide a justification of the individual's need to have access to SI;
- Have their nomination approved by Communication Intelligence Control Officer (COMCO);
- Have successfully completed a subject interview for Special Intelligence to compartmented intelligence, if any issue is raised in the interview that impacts the individual's loyalty or reliability as it relates thereto, CSIS is to be advised; a field investigation may be initiated to ascertain full details of this information;
- Be indoctrinated to SI Access; and
- Request renewal at the time of his/her Top Secret update (every 5 years).

In order to request an employee be indoctrinated to SI, management is responsible to complete this document and forward to CBSA COMCO who, upon approval, will forward it to the Manager, Personnel Security Screening Section.

**Management is also responsible to advise the COMCO (SI-IS@cbsa-asfc.gc.ca) if there is no longer a requirement for an employee to have access to SI. A de-indoctrination must be conducted and the employee's name be removed from the list of authorized personnel from Communications Security Establishment Canada.**

| | | | |
|---|---|---|---|
| Surname (Last name) | Full given names (no initials) underline or circle usual name used | PRI | |
| Signature | Title | | |
| Unit / Division / Directorate / Branch | Region | Email address | |
| Date of Birth (yyyy/mm/dd) | Place of Birth (City/Province/Country) | Citizenship (indicate if dual) | Employee's current security screening level - Effective date |

Provide justification for employee to require access to Special Intelligence (SI) (Course of duties, Special Project, Special Operation, etc)

Specify the reason for the requirement to SI

☐ In accordance with duties/position number ☐ Special Operations ☐ TLO/MIO

☐ Other (please specify) ______

Type of SI Access

☐ Read Only ☐ Customer Relation Officer (CRO) Services ☐ Secure Email ☐ SIGINT Secure Area (SSA)

I, the undersigned, certify that the employee must be indoctrinated to Special Intelligence I as per justification. I fully understand it is my responsibility to ensure that the employee is de-indoctrinated when there is no longer a requirement for the employee to have access to SI Information.

| | | |
|---|---|---|
| Name of Director General | Signature of Director General | Date (yyyy/mm/dd) |
| COMINT Control Officer (COMCO) or Deputy | Signature of COMCO or D-COMCO | Date (yyyy/mm/dd) |

BSF680 E (14)




Agence des services frontaliers du Canada | Canada Border Services Agency

**PROTÉGÉ B une fois rempli**

L'information fournie dans le présent formulaire, est collectée en vertu du paragraphe **7(1) de la *Loi sur la gestion des finances publiques*** et de ***la Politique de sécurité du gouvernement du Canada (PSG)***, est requise pour le contrôle de sécurité du personnel. Les renseignements recueillis peuvent aussi être divulgués à la Gendarmerie royale du Canada (GRC), au Service canadien du renseignement de sécurité (SCRS), et qui mèneront les vérifications ou les enquêtes nécessaires en vertu de la PSG, et aux entités à l'extérieur du gouvernement fédéral (comme des bureaux de crédit) aux fins du contrôle de sécurité du personnel.

Vous avez le droit d'accéder à vos renseignements personnels et/ou d'y apporter des corrections en vertu de l'article ***12 de la Loi sur la protection des renseignements personnels***. Les renseignements recueillis sont décrits dans le fichier des renseignements personnels du contrôle de sécurité du personnel ASFC PPU 1108 qui est présenté en détail sur le site www.infosource.gc.ca.

**Justification de l'endoctrinement initial ou mise à jour pour obtenir l'accès à des renseignements spéciaux (SI)**

Conformément à la Normes canadiennes sur la sécurité du SIGINT, Centre de la sécurité des télécommunications Canada, du, toute personne devant avoir un accès direct à des renseignements spéciaux (RS) ou à de l'information liée aux RS doit :
- Être parrainée par l'autorité du ministère qui en fait la demande au nom de la personne;
- Être de citoyenneté canadienne;
- Détenir une cote de sécurité de niveau très secret;
- Justifier la nécessité de l'accès à des RS;
- Avoir été nommée avec l'approbation de l'agent de surveillance du renseignement sur les communications (COMCO);
- Avoir réussi une entrevue dans le cadre des renseignements spéciaux liés à des renseignements compartimentés. Si toute question visant la loyauté ou la fiabilité de la personne à cet égard est soulevée au cours de l'entrevue, le Service canadien du renseignement de sécurité doit en être informé; une enquête sur place peut être effectuée pour obtenir plus de détails concernant ces renseignements;
- Être endoctriné pour accéder à des RS;
- Demander le renouvellement lors de la mise à jour de sa cote de sécurité de niveau très secret (tous les 5 ans).

Pour demander l'endoctrinement d'un employé aux fins d'accès aux RS, l'équipe de gestion doit remplir le présent document et le transmettre à l'agent de surveillance COMCO de l'ASFC, qui, dès son approbation, le transmettra au gestionnaire de l'Unité des enquêtes de sécurité sur le personnel.

**Lorsqu'un employé n'a plus besoin d'accéder aux RS, l'équipe de gestion doit en informer le COMCO, (SI-IS@cbsa-asfc.gc.ca). L'employé doit alors être dé-endoctriné et son nom doit être rayé de la liste des employés autorisés du Centre de la sécurité des télécommunications du Canada.**

| Nom (de famille) | Prénoms au complet (aucune initiale) souligné ou encerclé le prénom usuel | CIDP |
|---|---|---|
| | | |

| Signature | Titre |
|---|---|
| | |

| Unité / Division / Direction / Direction générale | Région | Adresse électronique |
|---|---|---|
| | | |

| Date de naissance (aaaa/mm/jj) | Lieu de naissance (Ville / Province / Pays) | Citizenship (indiquer si double) | Cote de sécurité actuelle de l'employé - date d'entrée en vigueur |
|---|---|---|---|
| | | | |

Donner la justification pour laquelle l'employé doit avoir accès à des renseignements spéciaux (RS) (accomplissement des fonctions, projet spécial, opération spéciale, etc.)

Précisez la raison pour laquelle l'accès aux RS est nécessaire

☐ Conformément aux tâches ou au numéro du poste ☐ Opérations spéciales ☐ Agent de liaison / Agent de liaison temporaire

☐ Autre (veuillez préciser) ____________________

Type d'accès aux RS

☐ Lecture seulement ☐ Services d'agents de relations avec la clientèle ☐ Courrier électronique sécurisé ☐ SIGINT Secure Area (SSA)

Je soussigné certifie que l'employé doit être endoctriné pour accéder à des renseignements spéciaux, conformément à la justification. Je comprends que j'ai la responsabilité de m'assurer que l'employé sera dé-endoctriné lorsqu'il n'aura plus besoin de l'accès à des renseignements spéciaux.

| Nom du directeur général | Signature directeur général | Date (aaaa/mm/jj) |
|---|---|---|
| Agent de surveillance COMCO ou délégué | Signature du COMCO ou délégué | Date (aaaa/mm/jj) |

BSF680 F (14)



Canada Border Services Agency / Agence des services frontaliers du Canada



# DIRECTIVE ON THE SECURITY OF SPECIAL INTELLIGENCE

PROTECTION • SERVICE • INTEGRITY





This directive takes effect on February 5, 2015.

## Scope

Some classified and sensitive information related to National intelligence interests has been identified and designated as **Special Intelligence (SI)**. Special Intelligence Material is all information and material that requires special control for restricted handling under compartmented foreign intelligence systems. It is equivalent to the United States' term Sensitive Compartmented Information (SCI). As an example, Special Material includes (but is not limited to) Signal Intelligence (SIGINT).

The Canada Border Services Agency (CBSA) has been named by the Communications Security Establishment Canada (CSEC) and its associated partner countries as a Canadian authorized organization approved to receive and retain Special Intelligence.

## Office of Primary Interest (OPI)

The OPI for all matters relating to the Security of Special Intelligence is the Communication Intelligence Control Officer (COMCO) in the Security and Professional Standards Directorate (SPSD). Any enquiries should be directed to the COMCO, SPSD (SI-IS@cbsa-asfc.gc.ca).

These instructions address the following topics:

| Topics |
|---|
| **Policy** |
| **Responsibilities** |
| **Departmental Instructions** |
| **Registries/Sub-Registries** |
| **Limited Access** |
| **SI Access Justification** |
| **Agency COMCO** |
| **SIGINT Secure Area (SSA)** |
| **Security Investigations and Reporting** |
| **Use of Special Intelligence** |
| **Contacts** |







## Policy

Special Material is vulnerable to easily applied methods of counterintelligence. For this reason, the Government of Canada (GC) requires and directs that special security measures be applied to this material to ensure its protection.

The Canadian SIGINT Security Standards (CSSS) published by the National SIGINT Authority, Communications Security Establishment Canada (CSEC) sets the baseline security requirements in regard to Special Intelligence information for all GC departments and agencies.

Special Intelligence shall be subjected to stringent security safeguards outlined in this instruction as well as those contained in the CSSS. These safeguards include specific requirements for access, custody, handling and transmission. The proper safeguarding of Special Intelligence within each Department or Agency shall be managed by the Communication Intelligence (COMINT) Control Officer (COMCO) and shall be accomplished through a system of registries, established for that purpose.

## Responsibilities

The Director General, Security and Professional Standards Directorate (SPSD) is the Departmental Security Officer (DSO) and the Senior Indoctrinated Official (SIO) for the CBSA and is responsible for the administration of Special Intelligence access, dissemination and security within the CBSA.

The COMCO and DCOMCOs are appointed by the SIO. The COMCO is located in SPSD and the Deputy COMCOs are located in each SIGINT Secure Area (SSAs). In addition to being responsible for the control of Special Intelligence, these appointees provide guidance to all CBSA Special Intelligence holders.

## Agency Instructions

Instructions for the custody, handling and transmission of Special Intelligence are contained in the SIGINT Secure Area Security Orders (SSA SO). These directives are issued under the authority of the SIO and apply to the CBSA Special Intelligence registry and all the indoctrinated personnel.







## Registries/Sub-Registries

The CBSA operates several central Special Intelligence (SI) registries. When the volume of SI is such that regular, detailed document accountability is impracticable (e.g. large volumes of material received in soft copy through an IT system), adequate records must be maintained of hard copies/or soft copies made on magnetic media, to ensure accountability.

A Deputy COMINT Control Officers (DCOMCO) is appointed for each Special Material sub-registry. Administratively, each sub-registry is responsible directly to the COMCO.

## Limited Access

Access to SI is limited to members cleared to the appropriate Top Secret Special Intelligence (TS SI) clearance level, and who have an absolute need-to-know. Those employees are included on an appropriate Special Intelligence Access List and have been specifically indoctrinated and thoroughly briefed on their responsibilities regarding the safeguarding of SI. Access to one category of SI does not automatically allow access to the other categories.

## Special Intelligence (SI) Access Justification

In accordance with the policy of Communication Security Establishment Canada, anyone who requires direct access to SI and Si-related information must:

- Be sponsored by an authority in the department requesting direct access to Special Intelligence on behalf of an individual;
- Be a Canadian Citizen;
- Hold a Top Secret security clearance;
- Provide a justification of the individual's need to have access to SI;
- Have their nomination approved by Communication Intelligence Control Officer (COMCO);
- Have successfully completed a subject interview for Special Intelligence to compartmented intelligence, if any adverse is raised in the interview that impacts the individual's loyalty or reliability as it relates thereto, CSIS is to be advised; a field investigation may be initiated to ascertain full details of this information;
- Be indoctrinated to SI Access; and
- Request renewal at the time of his/her Top Secret update (every 5 years).







In order to request an employee be indoctrinated to SI, management is responsible to complete the Justification for Initial or Update Indoctrinations to Special Intelligence (SI) Access, BSF680 and forward to CBSA COMCO (SI-IS@cbsa-asfc.gc.ca) who upon approval will forward it to the Manager, Personnel Security Screening Section.

Management is also responsible to advise the COMCO (SI-IS@cbsa-asfc.gc.ca) if there is no longer any requirement for an employee to have access to SI. A de-indoctrination must be conducted and the employee's name be removed from the list of authorized personnel from Communications Security Establishment Canada.

Security and Professional Standards directorate will review yearly the list of employees who had been granted SI access to ensure it is up to date and access is provided only on those with a need to know due to their functions/duties.

## COMCO

All supervisors are responsible to ensure that selected individuals hold the required indoctrination prior to being given access to a category of Special Intelligence. Requests or renewals for Special Intelligence clearances are to be directed to the CBSA COMCO in Ottawa.

## SIGINT Secure Area (SSA)

A SIGINT Secure Area (SSA) is an area, room, group of rooms or installation, which meets the physical security standards where SI may be stored, used, discussed and electronically or manually processed. A SSA is accredited by CSEC and can be permanent or temporary.

Specific direction and policy relating to the construction and operation of a SSA are available by contacting Physical Security and/or the COMCO.

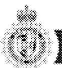
All SI shall be stored, used, discussed and electronically or manually processed inside an approved SSA.

In addition, discussions at that level, shall take place in a SSA or an approved Special Intelligence Secure Discussion Area (SDA).

All SI information management systems shall be certified and accredited by CSEC located in Ottawa.







Due to the need-to-know principle, swipe access to the SSA is limited to the employees of the Enforcement and Intelligence Operations Directorate, National Security Screening Division, Enforcement and Intelligence Programs Directorate, and senior management.

## Security Investigations and Reporting

The COMCO is responsible for the administration and control of the Special Intelligence security violation/breach program and for the maintenance of an appropriate register/log system.

All SI security violations/breaches (hard copy and electronic) shall be reported to the COMCO and duly investigated in accordance with CSEC Special Intelligence Policy Directives. Results of the investigation will be reported to the Departmental Security Officer (DSO).

## Use of Special Intelligence

Special Intelligence information may not be sanitized, downgraded or declassified without the approval of the originating authority. Any potential or actual use of SI in legal proceedings must be coordinated through the CBSA SIGINT Secure Area (SSA) or the COMCO, which in turn consults with the appropriate originating authority.

## Contacts

| | | |
|---|---|---|
| **SI Mail Box** | **General Inquiry** | CBSA-ASFC_SI-IS@cbsa-asfc.gc.ca |





Agence des services frontaliers du Canada | Canada Border Services Agency

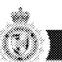


# Directive sur la sécurité des renseignements spéciaux

PROTECTION • SERVICE • INTÉGRITÉ



Agence des services frontaliers du Canada | Canada Border Services Agency



Cette directive entre en vigueur le 5 février, 2015.

## Portée

Certains renseignements classifiés et sensibles d'intérêt pour le renseignement national ont été définis et désignés comme **renseignements spéciaux (SI)**. Les SI représentent toute information ou tout document exigeant une surveillance particulière pour en garantir la manipulation restreinte, avec des systèmes de renseignements étrangers cloisonnés. Il s'agit d'un équivalent du terme « Sensitive Compartmented Information » (information sensible cloisonnée) utilisé aux États Unis. À titre d'exemple, les documents spéciaux comprennent (mais n'est pas limité à) notamment le renseignement d'origine électromagnétique (SIGINT).

L'Agence des services frontaliers du Canada (ASFC) a été désignée par le Centre de la sécurité des télécommunications Canada (CSTC) et ses pays partenaires comme un organisme canadien autorisé à recevoir et à conserver les renseignements spéciaux.

## Bureau de première responsabilité (BPR)

Le BPR en ce qui concerne toutes les affaires liées à la sécurité des renseignements spéciaux est l'agent de surveillance du renseignement sur les communications (COMCO) à la Direction de la sécurité et des normes professionnelles (DSNP). Toutes les demandes doivent être adressées au COMCO de la DSNP (CBSA-ASFC_SI-IS).

Les présentes instructions abordent les sujets suivants :



## Politique

Le matériel spécial est vulnérable aux méthodes de contre renseignement faciles à utiliser. Pour cette raison, le gouvernement du Canada exige l'adoption de mesures spéciales en matière de sécurité pour protéger ce genre de matériel.





Conformément aux normes canadiennes de sécurité en matière de SIGINT (NCSS) publiées par l'autorité nationale de SIGINT, le Centre de la sécurité des télécommunications Canada (CSTC) établit les exigences de base concernant la sécurité des renseignements spéciaux pour tous les organismes et ministères du gouvernement du Canada.

Les renseignements spéciaux doivent être protégés au moyen des mesures de sécurité rigoureuses décrites dans cette présente instruction et celles décrites dans les NCSS. Ces mesures comprennent des exigences précises touchant l'accès, la garde, le traitement et la transmission. La protection adéquate des renseignements spéciaux dans chaque ministère ou agence doit être gérée par l'agent de surveillance du renseignement sur les communications (COMCO) et doit être appliquée à l'aide d'un système de dépôts et de dépôts auxiliaires établi à cette fin.

## Responsabilités

Le directeur général de la Direction de la sécurité et des normes professionnelles (DSNP) est l'agent de sécurité du ministère (ASM) ainsi que le représentant formé principal (RFP) pour l'ASFC et il est responsable de l'administration des accès, de la diffusion et de la sécurité des renseignements spéciaux à l'ASFC.

Le COMCO et les COMCO adjoints sont nommés par le RFP. Le COMCO se trouve à la DSNP et les COMCO adjoints se trouvent dans chaque zone d'accès réservé SIGINT (ZARS). En plus d'être responsables du contrôle des renseignements spéciaux, ces personnes nommées offrent des conseils à tous les détenteurs de renseignements spéciaux à l'ASFC.

## Instructions de l'Agence

Les instructions relatives à la garde, au traitement et à la transmission des renseignements spéciaux figurent dans les ordres de sécurité de la zone d'accès réservé SIGINT (OS de la ZARS). Ces directives sont publiées avec l'autorisation du RFP et s'appliquent au dépôt de renseignements spéciaux de l'ASFC ainsi qu'à tout le personnel endoctriné.

## Dépôts et dépôts auxiliaires

L'ASFC exploite plusieurs dépôts centraux de renseignements spéciaux. Si la quantité de renseignements spéciaux est telle qu'il est impossible de faire un compte rendu régulier et détaillé des documents (p. ex., de grandes quantités de matériel reçues de façon électronique au moyen d'un système informatique), des registres adéquats des copies papier ou électroniques sur support magnétique doivent être tenus afin d'assurer la reddition de comptes.

Un agent adjoint de surveillance du renseignement sur les communications (COMCO adjoint) est nommé pour chaque sous registre de matériel spécial. Sur le plan administratif, chaque sous-registre relève directement du COMCO.

## Accès limité

L'accès aux renseignements spéciaux est limité à un nombre restreint de membres habilités au niveau Très secret/Renseignements spéciaux qui ont absolument besoin de connaître ces renseignements. Ces employés sont intégrés sur les listes d'accès aux renseignements et ont été spécialement endoctrinés et dûment informés sur leurs responsabilités relatives à la protection





des renseignements spéciaux. L'autorisation d'accès à une catégorie de renseignements spéciaux ne donne pas automatiquement accès aux autres catégories.

## Justification de l'accès aux renseignements spéciaux

Conformément à la politique du Centre de la sécurité des télécommunications Canada, quiconque a besoin d'un accès direct aux renseignements spéciaux ou à de l'information liée aux renseignements spéciaux doit :

- être parrainé par un responsable dans le ministère présentant la demande d'accès direct aux renseignements spéciaux au nom d'une personne;
- être citoyen canadien;
- avoir une cote de sécurité de niveau Très secret;
- fournir une justification du besoin d'accéder aux renseignements spéciaux;
- faire approuver sa nomination par l'agent de surveillance du renseignement sur les communications (COMCO);
- avoir réussi une entrevue personnelle pour les renseignements spéciaux dans le renseignement cloisonné, et si un élément défavorable pouvant avoir des conséquences sur sa loyauté ou sa fiabilité en ce qui concerne les renseignements spéciaux est relevé au cours de l'entrevue, le SCRS doit en être informé; une enquête peut alors être ouverte afin de vérifier tous les détails concernant cette information;
- être endoctriné sur l'accès aux renseignements spéciaux;
- demander un renouvellement de son accès au moment de la mise à jour de sa cote de sécurité de niveau Très secret (tous les 5 ans).

Pour demander qu'un employé soit endoctriné sur les renseignements spéciaux, la direction a la responsabilité de remplir le formulaire de justification de formation initiale ou de mise à jour de la formation sur l'accès aux renseignements spéciaux, BSF680 (PDF, 1.71 Mo), et de le faire parvenir au COMCO de l'ASFC (CBSA-ASFC SI-IS) qui, après approbation, l'enverra au gestionnaire de la Section des enquêtes de sécurité sur le personnel.

La direction a également la responsabilité d'informer le COMCO (CBSA-ASFC SI-IS) si un employé n'a plus besoin d'un accès aux renseignements spéciaux. Une procédure de retrait de l'accès doit être suivie, et le nom de l'employé doit être retiré de la liste des employés autorisés du Centre de la sécurité des télécommunications Canada.

La Direction de la sécurité et des normes professionnelles examinera chaque année la liste des employés auxquels on a accordé un accès aux renseignements spéciaux afin d'assurer qu'elles soient à jour et que cet accès est uniquement accordé aux personnes qui en ont besoin en raison de leurs fonctions ou de leurs tâches.

## COMCO de l'Agence

Tous les superviseurs doivent s'assurer que les personnes choisies suivent l'endoctrinement obligatoire avant de recevoir l'accès à une catégorie de renseignements spéciaux. Les demandes







ou les renouvellements d'autorisations d'accès aux renseignements spéciaux doivent être acheminés au COMCO de l'ASFC à Ottawa.

## Zone d'accès réservé SIGINT (ZARS)

Le terme « zone d'accès réservé SIGINT » (ZARS) désigne une zone, une pièce, un ensemble de pièces ou une installation qui respecte les normes de sécurité matérielle où les renseignements spéciaux peuvent être entreposés, utilisés, examinés, ainsi que traités manuellement ou électroniquement. Une ZARS est homologuée par le CSTC et peut être permanente ou temporaire.

Il est possible d'obtenir des instructions précises et des politiques concernant la construction et l'exploitation d'une ZARS en communiquant avec la Sécurité matérielle ou le COMCO.

Tous les renseignements spéciaux doivent être conservés, utilisés, discutés et traités, de façon électronique ou manuelle, à l'intérieur d'une ZARS approuvée.

De même, les discussions à ce niveau doivent se dérouler dans une ZARS ou un espace de discussion protégé approuvé pour les renseignements spéciaux.

Tous les systèmes de gestion des renseignements spéciaux doivent être certifiés et homologués par le CSTC d'Ottawa.

En raison du principe du besoin de connaître, l'accès par bande magnétique à la ZARS est limité aux employés de la Direction des opérations relatives à l'exécution de la loi et au renseignement, de la Division des enquêtes pour la sécurité nationale, de la Direction des programmes de l'exécution de la loi et du renseignement et à la haute direction

## Enquêtes et rapports de sécurité

Le COMCO est responsable de l'administration et du contrôle du programme d'infraction ou d'atteinte à la sécurité des renseignements spéciaux et de la tenue d'un système de journal ou de registre approprié.

Toutes les infractions et atteintes à la sécurité des renseignements spéciaux (copies papier ou électroniques) doivent être signalées au COMCO et doivent faire l'objet d'une enquête en bonne et due forme, conformément aux directives de la politique concernant les renseignements spéciaux du CSTC. Les résultats de l'enquête doivent être présentés à l'agent de sécurité du ministère (ASM).

## Utilisation des renseignements spéciaux

Les renseignements spéciaux ne peuvent pas être nettoyés, déclassés ou retirés sans l'approbation de l'auteur responsable. Toute utilisation réelle ou éventuelle des renseignements spéciaux dans des procédures judiciaires doit être coordonnée dans la zone d'accès réservé SIGINT de l'ASFC ou par l'entremise du COMCO qui consultera l'auteur responsable concerné.

## Personnes ressources






Agence des services frontaliers du Canada	Canada Border Services Agency

**Boîte aux lettres pour les renseignements spéciaux** : Demande de renseignements : CBSA-ASFC_SI-IS

PROTECTION • SERVICE • INTÉGRITÉ



Canada Border Services Agency | Agence des services frontaliers du Canada



Information Security

IT Security and Continuity Division

Enterprise Services Directorate

# Policy on Information Technology (IT) Security

PROTECTION SERVICE INTEGRITY INTÉGRITÉ PROTECTION SERVICE INTEGRITY INTÉGRITÉ PROTECTION SERVICE INTEGRITY INTÉGRITÉ PROTECTION SERVICE INTEGRITY

March 1, 2015

PROTECTION • SERVICE • INTEGRITY

Canada

PROTECTION • SERVICE • INTEGRITY

Canada

## Contents

# 1. EFFECTIVE DATE

This policy is effective March 1st, 2015.

# 2. CONTEXT

The Policy on Government Security (PGS) requires departments/agencies to design and implement security programs that will preserve the confidentiality, integrity and availability of Information Technology (IT), information assets and to ensure the continued delivery of IT services by developing and implementing policies, standards and guidelines.

# 3. APPLICATION

This policy is applicable to:

- All CBSA management and employees (permanent, term, casual, part-time), contract and private agency personnel, and individuals seconded or assigned to CBSA (including students) and any other individuals required to comply with CBSA policy by virtue of a contract or a memorandum of understanding (MOU).
- External service providers when they store or process CBSA IT information assets (e.g. Shared Service Canada)
- All IT information created, collected, stored, processed, transmitted or destroyed by information systems, information technology hardware and software, computer media, communications networks, telecommunications and related equipment and services.

# 4. AUTHORITIES

This policy is applicable in support of:

- Treasury Board - Framework for the Management of Risk
- Treasury Board - Policy on Government Security
- Treasury Board - Operational Security Standard: Management of Information Technology Security

# 5. POLICY STATEMENT

All CBSA IT information holdings, assets and services must be protected to ensure confidentiality, integrity and availability.

## 5.1. OBJECTIVE

Ensure effective IT Security practices are disseminated and utilized across the Agency to protect Agency electronic services, resources, and information.

## 5.2. EXPECTED RESULTS

The expected results of this policy are:

- Sound management and decisions, related to the design and development of IT information assets and services, in consideration of IT Security requirements; and
- Clear responsibilities in the CBSA for decision-making and effective administration of Policy on Government Security (PGS) in respect of IT Security.

# 6. REQUIREMENTS

The CBSA must:

- Ensure that access to IT information systems is controlled and managed;
- Ensure that users accessing Agency IT information systems are identified and authenticated;
- Ensure that risks associated with IT Systems are appropriately assessed and that mitigations are put in place or risk accepted by management in consultation with and approval of the Departmental Security Officer (DSO);
- Ensure access controls in IT information systems adequately protect information assets;
- Provide a secure computing environment; and
- Enforce acceptable use of the CBSA's electronic resources.

The following key principles must also guide IT security safeguards:

## 6.1. Need to know principle

Access to information is limited to users with the appropriate security screening level, and that users only have access to information and systems that are required to fulfill their duties. Even if users have the required conditions to access information (e.g. employment status, security clearance), they can only access and know information if and only if this is required for them to perform their duties. For instance, an employee with a Level II Secret clearance can only get access to a specific Classified Secret file if knowing this information is required to perform his/her duties.

## 6.2. Least privilege

Process or individual who has been given only the authority needed to accomplish the task and nothing more. For instance, an account to perform backup must be given read access to the information that must be backup. Extended rights such as modify/delete access and install new software (for example) must not be granted.

### 6.3. Segregation of duties

Segregation of duties refers to a process that is divided between different individuals in order to reduce the scope for error and fraud. For instance, an IT specialist designing an information system is not the same person tasked with assessing the security of that system.

### 6.4. Security throughout the system development life cycle

All programs and technology areas must ensure that IT security requirements are identified, assessed and implemented as an integral part of any design, development, implementation or an enhancement to any new or existing process or system.

Technology architecture and design must be documented at the time of completion of the design for IT Security assessment and such documentation must be maintained throughout the life of such technology.

All security products and tools (hardware and/or software) must be security evaluated prior to use. Additionally, these products or tools must be properly configured and operated to ensure that all security functions are effective.

All project management methodologies, development processes and technology architecture must incorporate the baseline security requirements, including policies and standards, identified for the Agency's systems and information as represented by Service Lifecycle Management Framework (SLMF).

## 7. ROLES, RESPONSIBILITIES AND ACCOUNTABILITY

### 7.1. Departmental Security Officer (DSO)

The DSO is responsible for:

- Providing consultation and approval in consideration of the acceptance of all security risks;
- Ensuring that the IT Security Program is included within the overall CBSA Security Program;
- Providing oversight of the Agency Security Program, including assuring the access to agency information is controlled appropriately;
- Investigating and responding to reports of non-compliance with this policy and ensuring that appropriate remedial actions are taken when/as required; and
- Providing input and feedback on the development of IT security policy instruments.

### 7.2. IT Security Coordinator (ITSC)

The ITSC is responsible for:

- Establishing and managing a departmental IT security program as part of a coordinated CBSA Security Program,
- Reviewing and recommending approval of departmental IT security policies and standards, and all policies that have IT security implications,
- Ensuring review of the IT security related portions of Request for Proposals and other contracting documentation, including Security Requirements Checklists,





- Recommending approval of all contracts for external providers of IT security services,
- Working closely with program and service delivery managers to ensure their IT security needs are met,
  - providing advice on safeguards,
  - advising them of potential impacts of new and existing threats, and
  - advising them on the residual risk of a program or service,
- Monitoring departmental compliance with Operational Security Standard: Management of Information Technology Security (MITS),
- Promoting IT security in the department,
- Establishing an effective process to manage IT security incidents, and monitor compliance with it,
- Serving as the department's principal IT security contact;
- Working with the Departmental Security Officer to ensure that physical, personnel and IT security stakeholders coordinate their efforts to protect information and IT assets and ensure an integrated, balanced approach;
- Working with the Chief Information Officer to ensure that appropriate security measures are applied to all departmental IM and IT assets, activities and processes;
- Providing guidance on the development and implementation of technical security specifications;
- Ensuring that CBSA patch management process is documented and followed to ensure security-related patches are applied in a timely manner and that this process is effective;
- Supporting the DSO on audit response to information security audits and co-ordinating all responses to technical security audit report issues and formulating management response;
- Ensuring that the Cyber Protection Centre meets required IT security safeguards to protect CBSA information;
- Working with the Business Continuity Planning Coordinator to ensure a comprehensive approach to continuous service delivery;
- Providing guidance to Operational Personnel in:
  - Following security procedures and recommend improvements to them,
  - Responding to security incidents,
  - Testing and installing security patches,
  - Maintaining or upgrade security hardware and software,
  - Monitoring systems and logs,
  - Back up and recover information, and
  - Managing access privileges and rights.

## 7.3. Regions and Branches

Regions and Branches are responsible for:

- Safeguarding all information and assets under their control including IT information and assets;
- Liaising with the DSO and ITSC on the interpretation of information security and technical security policies and standards;
- Advising and monitoring, in consultation with the ITSC, on the implementation of IT security within their local areas;
- Implementing IT security standards and guidelines;
- Conducting local management review and monitoring the implementation of inspection and audit recommendations;





- Maintaining awareness programs for IT security in support of operational requirements;
- Ensuring that independent security assessments are performed (by ITSC) on all IT information systems (including locally developed information systems);
- Supporting regional IT security audits with local office input and response;
- Reporting on IT security incidents, or suspected incidents;
- Ensuring that IT security requirements are included in contracts, RFPs and Security Requirements Checklists; and
- Ensuring that IT security is included in Written Collaborative Arrangements and Agreements via the participation, as required, of the DSO and the ITSC.

### 7.4. Individuals

All individuals entrusted with access, creation, maintenance, transport, release, protection and/or disposal of CBSA information are responsible to be aware of the requirements of the directive and must adhere to this directive by adequately applying the required IT security safeguards and by reporting deviations, or suspected deviations, from required safeguards.

## 8. COMPLIANCE AND REPORTING

The CBSA DSO, security practitioners and managers are responsible for monitoring compliance with this directive within CBSA, measuring the effectiveness of IT security safeguards and ensuring appropriate remedial actions are taken when deficiencies arise.

Individuals will report security incidents in accordance with the requirements outlined in the CBSA Security Manual, Norme de sécurité matérielle pour le signalement des incidents de sécurité.

## 9. CONSEQUENCES

The DSO is responsible for investigating and responding to reports of non-compliance with this directive and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies, directives or standards may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment.

## 10. DIRECTIVE REVIEW

The IT Security Coordinator (Director, IT Security and Continuity Division) should initiate a review of this directive at least every three years, or earlier as required.

# 11. REFERENCES

## 11.1. Treasury Board Secretariat

- TBS Policy on Government Security - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578
- TBS Directive on Departmental Security Management - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579
- TBS Operational Security Standard on Physical Security - https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329&section=text

## 11.2. Communications Security Establishment Canada

- CSEC Guidance ITSG-33 Annex 1 IT Security Risk Management: A Lifecycle Approach – Departmental IT Security Risk Management Activities - https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg33-ann1-eng_0.pdf
- CSEC Guidance ITSG-33 Annex 2 IT Security Risk Management: A Lifecycle Approach – Information System Security Risk Management Activities - https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg33-ann2-eng_1.pdf

## 11.3. Supporting IT Security Directives

- Directive on IT Security Risk Management
- Directive on Electronic Resources
- Directive on Computing Environment
- Directive on Identity Management
- Directive on IT Systems Access Control

# 12. ENQUIRIES

Enquiries regarding this directive should be directed to:

Information, Science and Technology Branch,
**Enterprise Services Directorate**
**IT Security and Continuity Division**

E-Mail: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca

Intranet : http://atlas/istb-dgist/services/it-ti-sec/it_ti_sec_eng.asp

Canada Border Services Agency | Agence des services frontaliers du Canada



Sécurité de l'information

Sécurité et continuité des opérations des TI

Direction des services organisationnels

# Politique sur la sécurité des technologies de l'information (TI)

1 mars 2015

PROTECTION • SERVICE • INTEGRITY

Canada



PROTECTION • SERVICE • INTÉGRITÉ

Canada

## Table des matières



# 1. DATE D'ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le 1er mars 2015.

# 2. CONTEXTE

Aux termes de la Politique du gouvernement sur la sécurité, les ministères et agences doivent concevoir et mettre en œuvre des programmes de sécurité qui garantiront la confidentialité, l'intégrité et la disponibilité des ressources liées aux technologies de l'information (TI) ainsi que veiller à une prestation continue des services de TI par l'élaboration et l'adoption de politiques, de normes et de directives.

# 3. CHAMP D'APPLICATION

La présente politique s'applique aux :

- membres de la direction et du personnel (permanents, nommés pour une période déterminée, occasionnels et à temps partiel) de l'Agence des services frontaliers du Canada (ASFC), aux employés contractuels et au personnel d'agence ainsi qu'aux personnes en détachement ou en affectation à l'ASFC, du fait d'un contrat ou d'un protocole d'entente (PE);
- aux fournisseurs de services externes lorsqu'ils stockent ou manipulent des ressources liées aux TI de l'ASFC (p. ex. Services partagés Canada);
- renseignements informationnels créés, recueillis, stockés, traités, transmis ou détruits au moyen de systèmes d'information, de matériel et d'un logiciel de technologie de l'information, d'un support informatique, de réseaux de communication, de moyens de télécommunications ou d'équipement et de services connexes.

# 4. RESPONSABLES

L'application de la présente politique vise à appuyer les mesures ci-après.

- Cadre stratégique de gestion du risque du Conseil du Trésor
- Politique sur la sécurité du gouvernement du Conseil du Trésor
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information du Conseil du Trésor

# 5. ÉNONCÉ DE POLITIQUE

L'ensemble des renseignements, des ressources et des services liés aux TI de l'ASFC doivent être protégés pour garantir leur confidentialité, leur intégrité et leur disponibilité.



### 5.1. OBJECTIF

Veiller à diffuser des pratiques efficaces de sécurité des TI et à les appliquer à l'échelle de l'Agence afin de protéger ses renseignements, ses ressources et ses services électroniques.

### 5.2. RÉSULTATS ESCOMPTÉS

Les résultats escomptés sont les suivants :

- Gestion et décisions judicieuses au chapitre de la conception et du développement des ressources informationnelles et des services de TI, sur la base des exigences en matière de sécurité des TI;
- Définition précise des responsabilités au sein de l'ASFC relativement au processus décisionnel et à l'administration efficace de la Politique sur la sécurité du gouvernement en ce qui concerne la sécurité des TI.

## 6. EXIGENCES

L'ASFC doit :

- contrôler et gérer l'accès aux systèmes informatiques;
- s'assurer qu'il y a identification et authentification des utilisateurs qui accèdent aux systèmes informatiques de l'Agence;
- veiller à l'analyse adéquate du risque associé aux systèmes informatiques et à la prise de mesures d'atténuation ou à l'acceptation du risque par la direction, sous réserve de consultation avec l'agent de sécurité du ministère (ASM) et de son approbation;
- vérifier que le contrôle de l'accès des systèmes informatiques protège comme il se doit les ressources informationnelles;
- garantir un environnement informatique sécuritaire;
- prescrire l'utilisation acceptable des ressources électroniques de l'ASFC.

Les principes fondamentaux suivants doivent également s'intégrer aux contrôles de sécurité des TI.

### 6.1. Principe du besoin de connaître

L'accès aux renseignements est limité aux utilisateurs possédant le niveau d'attestation de sécurité approprié, et les utilisateurs ont accès à l'information et aux systèmes que dans la mesure requise pour accomplir leurs tâches. Même si les utilisateurs répondent aux critères applicables pour accéder aux renseignements (p. ex. en vertu de leurs conditions d'emploi ou de leur cote de sécurité), ils seront autorisés à le faire et à prendre connaissance des renseignements uniquement si cela est nécessaire





dans le cadre de leurs fonctions. Par exemple, un employé ayant une cote de sécurité de niveau II (Secret) pourra accéder à un dossier classifié Secret précis que s'il a besoin de connaître les renseignements qu'il renferme pour exercer ses fonctions.

### 6.2. Droit d'accès minimal

Processus ou personne qui dispose seulement de l'accès nécessaire pour accomplir la tâche et rien de plus. Par exemple, un compte qui servirait à la sauvegarde doit avoir accès aux renseignements à sauvegarder en mode lecture seulement. Aucun autre droit, comme la modification ou la suppression des accès et l'installation de nouveaux logiciels, ne doit être accordé.

### 6.3. Séparation des tâches

La séparation des tâches s'entend d'un processus divisé entre différentes personnes dans le but de réduire la portée des erreurs et la fraude. Par exemple, l'évaluation de la sécurité d'un système ne sera pas menée par le spécialiste des TI qui a créé le système d'information en question.

### 6.4. Sécurité dans l'ensemble du cycle de développement des systèmes

À l'échelle des programmes et des domaines technologiques, la détermination, l'évaluation et l'application des exigences de sécurité des TI doivent faire partie intégrante de la conception, du développement et du déploiement de tout système ou processus ou de l'amélioration d'un système ou d'un processus.

L'architecture et la conception technologiques seront consignées au moment de l'élaboration aux fins d'évaluation de la sécurité des TI, et cette preuve sera conservée pendant toute la durée de vie de la technologie en question.

Une évaluation de la sécurité des outils et des produits de sécurité (matériel ou logiciel) doit avoir lieu avant l'utilisation de ces derniers. Aussi, la configuration et l'utilisation de ces outils ou produits doivent garantir l'efficacité des fonctions de sécurité.

Les méthodes de gestion de projets, les processus de développement et l'architecture technologique doivent intégrer les exigences de sécurité de base, y compris les politiques et normes applicables aux systèmes et renseignements de l'Agence selon le Cadre de gestion de cycle de la durée utile du service (CGCDS).

## 7. RÔLES, RESPONSABILITÉS ET REDDITION DE COMPTES

### 7.1. Agent de sécurité du ministère (ASM)

L'ASM doit :

- donner des conseils et son approbation quant au risque de sécurité connu;



- veiller à ce que le programme de sécurité des TI soit inclus dans le programme général de sécurité de l'ASFC;
- assurer la surveillance du programme général de sécurité de l'Agence, y compris en assurant que l'accès à l'information de l'agence est contrôlée de façon appropriée;
- enquêter et intervenir à la suite de signalements de cas de non-conformité à la présente politique et vérifier que les mesures correctives appropriées sont prises au moment opportun et selon les besoins;
- fournir des commentaires et de la rétroaction concernant l'élaboration d'instruments stratégiques en matière de sécurité des TI.

## 7.2. Coordonnateur de la sécurité des TI (CSTI)

Le CSTI doit :

- établir et gérer un programme ministériel de sécurité des TI dans le cadre d'un programme de sécurité coordonné de l'ASFC;
- examiner les politiques et normes ministérielles sur la sécurité des TI et toutes les politiques qui peuvent avoir des répercussions sur la sécurité des TI, et recommander leur approbation;
- veiller à la révision des sections portant sur la sécurité des TI dans les demandes de propositions et autres documents contractuels, incluant les listes de vérification des exigences relatives à la sécurité;
- recommander l'approbation de tous les contrats visant des fournisseurs externes des services de sécurité des TI;
- collaborer étroitement avec les gestionnaires de la prestation de programmes et services afin de veiller à ce que leurs besoins en sécurité des TI soient satisfaits, c'est-à-dire :
  - fournir des conseils sur les mesures de protection,
  - les conseiller sur les incidences éventuelles des menaces existantes et nouvelles,
  - les informer sur le risque résiduel lié à un programme ou service;
- surveiller la conformité du Ministère avec la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI);
- promouvoir la sécurité des TI au Ministère;
- établir un processus efficace pour gérer les incidents de la sécurité des TI et en surveiller la conformité;
- servir de principale personne-ressource au Ministère en qui a trait à la sécurité des TI;
- collaborer avec l'ASM afin de veiller à ce que les personnes responsables de la sécurité matérielle, de la sécurité du personnel et de la sécurité des TI coordonnent leurs efforts en vue de protéger les renseignements et les biens liés aux TI et favorisent une démarche intégrée et équilibrée;
- travailler avec le dirigeant principal de l'information pour s'assurer que les mesures de sécurité appropriées sont appliquées à l'ensemble des biens, des activités et des processus de GI et de TI du Ministère;
- prodiguer des conseils sur le développement et la mise en œuvre des spécifications de sécurité technique;

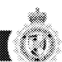


- vérifier que le processus de gestion des programmes de correction de l'ASFC est documenté et suivi afin de garantir la prompte activation des programmes de correction de sécurité et l'efficacité du processus;
- appuyer l'ASM relativement aux commentaires à la suite d'une vérification de la sécurité des renseignements et à la coordination de toutes les interventions à l'égard des problèmes mentionnés dans le rapport de vérification de la sécurité technique ainsi que formuler la réponse à la direction;
- s'assurer que le centre de cyberprotection emploie les contrôles de sécurité des TI requis pour protéger les renseignements de l'ASFC;
- travailler avec le coordonnateur de la planification de la continuité opérationnelle pour assurer une approche complète à la prestation continue des services;
- offrir des conseils au personnel opérationnel au chapitre :
    - du respect des procédures de sécurité, tout en recommandant des améliorations,
    - des mécanismes d'intervention lors d'incidents de sécurité,
    - de la mise à l'essai et de l'installation des programmes de correction,
    - de la mise à jour ou à niveau du matériel et du logiciel de sécurité,
    - de la surveillance des systèmes et des registres,
    - de la sauvegarde et de la récupération des renseignements,
    - de la gestion des privilèges et des droits d'accès.

## 7.3. Régions et directions générales

Les régions et les directions générales doivent :

- protéger tous les renseignements et les biens sous leur contrôle, y compris les renseignements et les ressources liés aux TI;
- agir comme personne-ressource auprès de l'ASM et du CSTI en ce qui concerne l'interprétation des politiques et des normes sur la sécurité des renseignements et la sécurité technique;
- donner des conseils, en collaboration avec le CSTI, sur la mise en œuvre de la sécurité des TI dans la région ainsi que surveiller ce déploiement;
- adopter des normes et des directives sur la sécurité des TI;
- procéder à un examen local de la gestion et surveiller l'application des recommandations découlant d'une inspection ou d'une vérification;
- maintenir des programmes de sensibilisation à la sécurité des TI en appui aux exigences opérationnelles;
- veiller à ce que des évaluations indépendantes de la sécurité (par le CSTI) aient lieu à l'égard de tous les systèmes informatiques (y compris les systèmes créés localement);
- apporter leur soutien aux vérifications régionales de la sécurité des TI (commentaires et réponses) par l'intermédiaire du bureau régional;
- produire des rapports sur les incidents de la sécurité des TI ou sur les incidents soupçonnés;
- vérifier que les exigences en matière de sécurité des TI sont incluses dans les contrats, les demandes de propositions et les listes de vérification des exigences relatives à la sécurité;



- s'assurer que la sécurité des TI est incluse dans les ententes et les accords de collaboration écrits, notamment par l'intermédiaire de la participation, au besoin, de l'ASM et du CSTI.

### 7.4. Personnes

Toutes les personnes autorisées à accéder à des renseignements et responsables de leur création, de leur mise à jour, de leur manipulation, de leur divulgation, de leur protection et de leur suppression sont responsables d'être au courant des exigences de la directive et doivent se conformer aux présentes en faisant adéquatement appel aux contrôles de sécurité des TI pertinents et en signalant tout écart, réel ou soupçonné, par rapport à ceux-ci.

## 8. CONFORMITÉ ET RAPPORTS

L'ASM de l'ASFC, le personnel de sécurité et les gestionnaires doivent surveiller la conformité aux présentes à l'échelle de l'Agence, mesurer l'efficacité des contrôles de sécurité des TI et prendre des correctifs appropriés lorsque des irrégularités se produisent.

Les incidents de la sécurité seront signalés selon les exigences énumérées dans le manuel sur la sécurité de l'ASFC, intitulé Norme de sécurité matérielle pour le signalement des incidents de sécurité.

## 9. CONSÉQUENCES

L'ASM doit enquêter et intervenir à la suite de signalements de cas de non-conformité aux présentes et vérifier que les mesures correctives appropriées sont prises au moment opportun et selon les besoins. Tout employé reconnu coupable d'avoir enfreint des politiques, des directives ou des normes s'expose à une entrevue motivée de filtrage de sécurité ainsi qu'à des mesures disciplinaires pouvant mener au congédiement.

## 10. EXAMEN DE LA DIRECTIVE

Le coordonnateur de la sécurité des TI (directeur, Sécurité et continuité des opérations des TI) doit entreprendre l'examen de cette directive au moins une fois au trois ans, ou plus fréquemment au besoin.







# 11. RÉFÉRENCES

## 11.1. Secrétariat du Conseil du Trésor

- Politique sur la sécurité du gouvernement du Sécrétariat du Conseil du Trésor du Canada (SCT) – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=16578
- Directive sur la gestion de la sécurité ministérielle du SCT – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16579
- Norme opérationnelle sur la sécurité matérielle du SCT – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329&section=text

## 11.2. Centre de la sécurité des télécommunications (CSTC)

- Annexe 1, Activités de gestion des risques liés à la sécurité des TI, du document d'orientation ITSG-33 du CSTC, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsg33-ann1-fra_0.pdf
- Annexe 2, Activités de gestion des risques liés à la sécurité des systèmes d'information, du document d'orientation ITSG-33 du CSTC, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsg33-ann2-fra_1.pdf

## 11.3. Directives connexes en matière de sécurité des TI

- Directive sur la gestion du risque en matière de sécurité des TI
- Directive sur l'utilisation des ressources électroniques
- Directive sur l'environnement informatique
- Directive sur la gestion de l'identité
- Directive sur le contrôle de l'accès aux systèmes de TI

# 12. DEMANDES DE RENSEIGNEMENTS

Veuillez adresser toute demande de renseignements au sujet des présentes à la :

| |
|---|
| Direction générale de l'information, des sciences et de la technologie<br>**Direction des services organisationnels**<br>**Sécurité et continuité des opérations des TI** |

Courriel : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Intranet : http://atlas/cb-dgc/sec/index_f.asp

Canada Border Services Agency | Agence des services frontaliers du Canada



# Directive for Access Control in Information Systems

January 20, 2015

PROTECTION • SERVICE • INTEGRITY



Canada Border Services Agency | Agence des services frontaliers du Canada



## Contents



# 1. EFFECTIVE DATE

This standard is effective January 20, 2015.

# 2. DIRECTIVE STATEMENT

## 2.1. Objective

Ensure that the management of assignment of access privileges to the Agency's IT networks/systems and information and the "need-to-know" and "least privilege" principles are maintained.

It is also closely related to the Directive for Identification and Authentication in Information Systems.

## 2.2. Expected Results

The expected results of this directive are:

a) Access control is an integral component of all CBSA programs, activities and services;
b) Only authorized *entities* with proper security clearance and a need to know are granted access to CBSA information systems;
c) Processes are established and effectively managed for maintaining system access permissions;
d) Access to Agency systems and information is monitored; and
e) Unauthorized access, disclosure, destruction, removal, modification and misuse of CBSA systems and information are mitigated.

# 3. APPLICATION

This directive applies to:

a) Employees of the Canada Border Services Agency (CBSA) and to any other individuals required to comply with CBSA policy by virtue of a contract or a memorandum of understanding (MOU); and
b) All entities requiring access to the Agency's IT networks/systems and information.

# 4. CONTEXT

The Policy on Government Security requires the *assurance* that information, assets and services are protected against compromise.

The Operational Security Standard: Management of Information Technology Security (MITS) Section 16 Prevention, Subsection 16.4 Technical Safeguards, Sub-subsection 16.4.3 Authorization and Access Control further mandates that:

a) Departments must restrict IT and information access to entities who have been security screened, authorized and approved; and have a "need to know" (Ref MITS 16.4.3);
b) Departments must keep access to the minimum required for individuals to perform their duties (i.e., the Principle of *least privilege*), and ensure that they are regularly updated to accurately reflect the current responsibilities of the individual (Ref MITS 16.4.3);







c) Departments must withdraw access privileges from individuals (including students, contractors, or others with short-term access as well as users on-long term absences such as secondment, maternity leave, etc.) who leave the organization, and revise access privileges when individuals move to jobs that do not require the same level of access (Ref MITS 16.4.3); and

d) Departments must screen, to at least the Secret level, all personnel with privileged access to critical systems (Ref MITS 16.3).

This directive is intended to be read in concert with the associated CBSA Directive for Identity Management and Authentication in Information Systems.

# 5. REQUIREMENTS

a) All access to systems, applications and services must adhere to this Directive for Access Control in Information Systems;

b) Access control is an integral component of all CBSA programs, activities and services;

c) Users are to be granted access privileges to the Agency's IT network/systems and information to perform assigned work-related activities and these privileges are not to be used for curiosity or personal gain;

d) Access privileges are to provide access only to the minimum amount and type of information the user requires for their duties (the "need-to-know" and "least-privilege" principles);

e) *Segregation of duties* is used when more than one user is required to perform a task;

f) Processes are established and effectively managed for maintaining system access permissions;

g) All users who require privileged access to critical systems must be cleared to the Secret level;

h) Privileged access to users will be granted for a period of 180 days at which time the privilege access request must be resubmitted, if necessary; and

i) Unauthorized access, disclosure, destruction, removal, modification and misuse of CBSA systems and information are mitigated.

# 6. ROLES AND RESPONSIBILITIES

## 6.1. Departmental Security Officer (DSO)

The DSO is responsible for:

- Oversight and control of the Agency's Access Control program;
- Ensuring access control requirements in this directive and supporting standard(s) and guidelines are implemented Agency-wide;
- Ensuring that security controls related to access control are included in security controls domain profiles;
- Assisting with developing and approving the Security Requirements Checklist (SRCL) for external organizations who require access to CBSA systems and resources;
- Reviewing and approving requests for access to external systems or services;
- Monitoring and reporting on the effectiveness of the Access Control Directive;
- Ensuring all users who require access to critical systems have the required Secret clearance;
- Determining the access control requirements for any system classified above Protected B.







## 6.2. IT Security Coordinator (ITSC)

The ITSC is responsible for:

- Assisting with embedding security controls related to access controls in security controls domain profiles;
- Assisting PSDMs with defining adequate access controls for their information systems;
- Ensuring security risks related to access control are assessed as part of information systems security risk assessments; and
- Providing security briefings to the CBSA user community related to access controls.

## 6.3. Program and Service Delivery Managers (PSDMs)

PSDMs are responsible for:

- Ensuring that the sensitivity of information contained in their information systems is defined;
- Ensuring access control requirements for the system are implemented commensurate with the sensitivity of the information;
- Determining privilege user requirements for the system;
- Identifying privileged users of the system;
- Identifying and authorizing users who have "privileged user" requirements to ensure that the assigned functions are in line with the user's work-related tasks; and
- Ensuring that their information systems maintain a record of system access privileges for each user (i.e. profiles, applications, administration privileges, etc.).

## 6.4. Users

Users are responsible for:

- Complying with the requirements of this directive and all related corporate policy instruments.
- All access activity associated with their user ID and exercise due diligence to protect CBSA information, systems, computers, and related devices from unauthorized use, access, disclosure, alteration or destruction;
- Attending security briefings related to access control, as required;
- Informing their manager when system access permissions are no longer required to perform current work related duties; and
- Safeguarding their credentials to protect access to information systems.

## 6.5. Managers

Managers are responsible for:

- Determining and identifying the minimum system access permissions for each employee to perform their-work related duties following the principles of need-to-know and segregation of duties;
- Approving or denying requests to suspend, reactive and/or withdraw employee system access permissions and adhere to established procedures;







- Ensuring that users who require privileged access to critical systems are screened to at the Secret level;
- Ensuring that user privileged access to critical systems users will be granted access for a period of 180 days at which time the requests to be designated a privileged user will be resubmitted, if necessary;
- Providing employees with only the minimum system access permission required to perform their specific work related duties;
- Ensuring that user access privileges are kept current and are to advise the local IT and / or security administrator when the access requirements change or are no longer required;
- Identifying and authorizing users who have "privileged user" requirements to ensure that the assigned functions are in line with the user's work-related tasks;
- Maintaining a record of all system accesses for each employee to facilitate monitoring and maintenance of system access permissions;
- Taking appropriate action to immediately suspend employee system access permissions if there is suspected misuse of information or breach of a related corporate policy instrument;
- Ensuring that changes to access control are implemented as required by following processes and performing tests (e.g. termination of employment, change in functions, extended leave - where the leave period exceeds 60 consecutive days, transfer, on-loan);
- Reviewing user access privileges at least semi-annually to ensure that the accesses to the Agency's IT networks/systems and information are in accordance with assigned work-related activities; and
- Immediately notify designated personnel in the Information Security Division of any suspected misuse of information or breach of this directive.

# 7. COMPLIANCE AND REPORTING

CBSA is responsible for ensuring that its programs and services are well managed. The Security and Professional Standards Directorate and the IT Security and Continuity Division must actively monitor management practices and controls related to this directive. Where significant deficiencies are encountered or improvements are needed, Agency senior officials will be informed.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Volume - Standards for Security Incident Reporting.

# 8. CONSEQUENCES

The DSO is responsible for investigating and responding to reports of non-compliance with this directive and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies; directives or standards may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment.







## 8.1. Directive Review

The IT Security Coordinator (Director ITSD) should initiate a review of this directive at least every three years, or earlier as required.

# 9. REFERENCES

**Treasury Board Secretariat (TBS)**

- *Policy on Government Security*
- Guideline on Defining Authentication Requirements - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=text
- Standard on Identity and Credential Assurance - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776&section=text
- Directive on Identity Management - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577&section=text
- Cyber Authentication Technology Solutions -Interface Architecture and Specification - Version 2.0 – https://kantarainitiative.org/confluence/download/attachments/45059378/CA%20-%20CATS%20IAS%20V2.0_Deployment%20Profile_Final%20r7.2_en.pdf?api=v2

**Communications Security Establishment Canada (CSEC)**

- IT Security Guidance: User Authentication Guidance for IT Systems - http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html

# 10. ENQUIRIES

Enquiries regarding this Directive should be directed to:

| Office Responsible | Contact Information |
|---|---|
| **Information, Science & Technology Branch**<br>IT Security & Continuity Division | **E-mail**: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca<br>**Intranet**: IT Security |
| **Comptrollership Branch**<br>Security and Professional Standards Directorate | **E-mail**: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca |





# 11. DEFINITIONS

Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive sur le contrôle de l'accès aux systèmes d'information

20 janvier 2015

PROTECTION • SERVICE • INTÉGRITÉ





# Table des matières









# 1. DATE D'ENTRÉE EN VIGUEUR

La présente norme entre en vigueur le 20 janvier 2015.

# 2. ÉNONCÉ DE LA DIRECTIVE

## 2.1. Objectif

S'assurer que la gestion de l'attribution des privilèges d'accès aux réseaux/systèmes de TI et aux renseignements de l'Agence ainsi que les principes du « besoin de connaître» et du « droit d'accès minimal » sont respectés.

En outre, la directive est étroitement liée à la Directive sur l'identification et l'authentification dans les systèmes d'information.

## 2.2. Résultats attendus

Les résultats attendus à l'égard de la présente directive sont les suivants :

a) Le contrôle de l'accès fait partie intégrante de l'ensemble des programmes, des activités et des services de l'ASFC.
b) Seules les *entités* autorisées disposant d'une cote de sécurité adéquate et jouissant d'un besoin de connaître ont la permission d'accéder aux systèmes d'information de l'ASFC.
c) Des processus sont établis et gérés efficacement pour tenir à jour la liste des permissions d'accès aux systèmes.
d) L'accès aux systèmes et aux renseignements de l'Agence est surveillé.
e) L'accès non autorisé aux systèmes et aux renseignements de l'ASFC de même que la divulgation, la destruction, l'élimination, la modification et l'usage abusif de ces derniers sont atténués.

# 3. APPLICATION

La présente directive s'applique :

a) aux employés de l'Agence des services frontaliers du Canada (ASFC) et à toute autre personne tenue de se conformer à la politique de l'ASFC en vertu d'un contrat ou d'un protocole d'entente (PE);
b) à toutes les entités qui doivent accéder aux réseaux/systèmes de TI et aux renseignements de l'ASFC.

# 4. CONTEXTE

La Politique sur la sécurité du gouvernement exige l'*assurance* que l'information, les biens et les services ne sont pas compromis.

Les points 16 Prévention, 16.4 Mesures de protection techniques et 16.4.3 Autorisation et contrôle de l'accès de la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) prévoient également que :







a) les ministères doivent limiter l'accès des TI et de l'information aux personnes qui ont fait l'objet d'une enquête de sécurité et qui ont été autorisées; qui ont été identifiées et authentifiées; et qui ont un besoin de connaître (GSTI 16.4.3);

b) les ministères ne doivent accorder que des privilèges d'accès minimums de manière à ce que les personnes ne puissent accomplir avec ceux-ci que les tâches liées à l'exercice de leurs fonctions (c.-à-d. en principe du droit d'accès minimal) et veiller à ce que les privilèges d'accès soient mis à jour régulièrement pour correspondre exactement aux responsabilités actuelles de la personne (GSTI 16.4.3);

c) les ministères doivent retirer les privilèges d'accès à toute personne (y compris les étudiants, entrepreneurs et autres personnes possédant un droit d'accès à court terme de même que les utilisateurs qui sont absents pour une période prolongée, comme un détachement, un congé de maternité, etc.) qui quitte l'organisation, et revoir les privilèges d'accès lorsque des personnes sont mutées à un poste qui ne requiert pas le même niveau d'accès (GSTI 16.4.3);

d) les ministères doivent effectuer une enquête de sécurité au moins jusqu'au niveau secret de tout membre du personnel ayant un accès privilégié aux systèmes essentiels (GSTI 16.3).

La présente directive est destinée à être lue parallèlement à la Directive relative à la gestion de l'identité et à l'authentification dans les systèmes d'information de l'ASFC.

# 5. EXIGENCES

a) Tous les accès aux systèmes, applications et services doivent être conformes à la présente Directive sur le contrôle de l'accès aux systèmes d'information;

b) le contrôle de l'accès fait partie intégrante de l'ensemble des programmes, des activités et des services de l'ASFC;

c) les privilèges d'accès aux réseaux/systèmes de TI et à l'information de l'Agence sont consentis aux utilisateurs pour qu'ils puissent effectuer les activités reliées au travail qui leur est assigné, et non pour satisfaire leur curiosité ou pour réaliser un gain personnel;

d) les privilèges d'accès doivent donner accès uniquement à l'information minimale dont l'utilisateur a besoin pour l'exercice de ses fonctions (principes de l'accès sélectif et du besoin de connaître minimal);

e) la *répartition des tâches* est utilisée lorsque plus d'un utilisateur est requis pour accomplir une tâche;

f) des processus sont établis et gérés efficacement pour tenir à jour la liste des permissions d'accès aux systèmes;

g) tous les utilisateurs qui ont besoin d'un accès privilégié aux systèmes essentiels doivent détenir une autorisation de sécurité de niveau secret;

h) les droits d'accès privilégié accordés aux utilisateurs sont valides pour une période de 180 jours, au terme de laquelle une nouvelle demande d'accès privilégié doit être présentée, au besoin;

i) l'accès non autorisé aux systèmes et à l'information de l'ASFC ainsi que la divulgation, la destruction, l'élimination, la modification et l'usage abusif de ces derniers sont atténués.



# 6. RÔLES ET RESPONSABILITÉS

## 6.1. Agent de sécurité du ministère (ASM)

L'ASM doit :

- surveiller et gérer le programme de contrôle de l'accès de l'Agence;
- s'assurer que les exigences en matière de contrôle de l'accès dans la présente directive et les normes et lignes directrices à l'appui sont mises en œuvre à l'échelle de l'Agence;
- s'assurer que des contrôles de sécurité liés au contrôle de l'accès sont inclus dans les profils de domaine des contrôles de sécurité;
- contribuer à l'élaboration et à l'approbation de la Liste de vérification des exigences relatives à la sécurité (LVERS) pour les organisations externes qui ont besoin d'avoir accès aux systèmes et aux ressources de l'ASFC;
- examiner et approuver les demandes d'accès aux systèmes ou aux services externes;
- surveiller l'efficacité de la Directive sur le contrôle de l'accès et rendre des comptes à cet égard;
- veiller à ce tous les utilisateurs qui ont besoin d'un accès aux systèmes essentiels disposent de l'autorisation de sécurité de niveau secret requise;
- déterminer les exigences en matière de contrôle de l'accès à l'égard de tout système classifié au-delà de Protégé B.

## 6.2. Coordonnateur de la sécurité des TI (CSTI)

Le CSTI doit :

- aider à enchâsser des contrôles de sécurité liés aux contrôles de l'accès dans les profils de domaine des contrôles de sécurité;
- aider les gestionnaires de l'exécution des programmes et de la prestation des services (GEPPS) à définir les contrôles d'accès adéquats à l'égard de leurs systèmes d'information;
- s'assurer que les risques en matière de sécurité liés au contrôle de l'accès sont évalués dans le cadre des évaluations des risques en matière de sécurité des systèmes d'information;
- donner des séances d'information en matière de sécurité à la communauté d'utilisateurs de l'ASFC relativement aux contrôles de l'accès.

## 6.3. Gestionnaires de l'exécution des programmes et de la prestation des services (GEPPS)

Les GEPPS doivent :

- s'assurer que la nature délicate de l'information contenue dans leurs systèmes d'information est définie;
- s'assurer que les exigences en matière de contrôle de l'accès aux systèmes sont mises en œuvre tout en tenant compte de la nature délicate de l'information;
- déterminer les besoins des utilisateurs privilégiés à l'égard du système;
- identifier les utilisateurs privilégiés du système;







- déterminer qui sont les utilisateurs ayant des besoins « d'utilisateur privilégié » et les autoriser pour s'assurer que les fonctions assignées correspondent aux fonctions de l'utilisateur;
- s'assurer que leurs systèmes d'information tiennent un registre des privilèges d'accès aux systèmes pour chaque utilisateur (p. ex. profils, applications, privilèges d'administration, etc.).

## 6.4. Utilisateurs

Les utilisateurs doivent :

- se conformer aux exigences de la présente directive et à tous les instruments de politique de l'Agence;
- assumer la responsabilité de toutes les activités d'accès associées à leur identificateur d'utilisateur et faire preuve d'une diligence raisonnable pour protéger l'information, les systèmes, les ordinateurs et les appareils connexes de l'ASFC contre l'utilisation, l'accès, la divulgation, la modification ou la destruction non autorisé;
- assister aux séances d'information en matière de sécurité concernant le contrôle de l'accès, au besoin;
- mettre leur gestionnaire au courant lorsque des permissions d'accès au système ne sont plus nécessaires pour l'exercice de leurs fonctions actuelles;
- protéger leurs justificatifs pour protéger l'accès aux systèmes d'information.

## 6.5. Gestionnaires

Les gestionnaires doivent :

- déterminer et définir le type de permission d'accès aux systèmes minimale nécessaire pour que chaque employé puisse exercer ses fonctions selon le principe du besoin de connaître et de la répartition des tâches;
- approuver ou refuser les demandes de suspension, de réactivation et/ou de retrait de permissions d'accès au système d'un employé et suivre les procédures établies;
- s'assurer que les utilisateurs ayant besoin d'un accès privilégié aux systèmes essentiels ont une cote de sécurité de niveau secret;
- s'assurer que l'accès privilégié de l'utilisateur aux systèmes essentiels est accordé pour une période de 180 jours, après quoi une nouvelle demande pour être désigné comme un utilisateur privilégié est soumise, au besoin;
- fournir aux employés la permission d'accès minimale requise aux systèmes pour l'exercice de leurs fonctions;
- s'assurer que les privilèges d'accès des utilisateurs sont tenus à jour et informer l'administrateur local de la sécurité et/ou de la TI lorsque des besoins liés à l'accès changent ou lorsque l'accès n'est plus requis;
- identifier et autoriser les utilisateurs ayant des besoins « d'utilisateur privilégié » pour s'assurer que les fonctions assignées correspondent aux fonctions de l'utilisateur;
- tenir à jour un registre de tous les accès aux systèmes de chaque employé pour faciliter la surveillance et la gestion des permissions d'accès aux systèmes;







- prendre des mesures appropriées pour suspendre immédiatement les permissions d'accès aux systèmes d'un employé s'il est soupçonné de faire un usage abusif de l'information ou de contrevenir à un instrument stratégique connexe de l'Agence;
- s'assurer que les changements touchant les contrôles d'accès sont mis en œuvre conformément aux processus et font l'objet d'essais (p. ex. cessation d'emploi, changement de fonction, congé prolongé – lorsque la période de congé excède 60 jours consécutifs, transfert, détachement);
- examiner les privilèges d'accès des utilisateurs au moins tous les six mois pour s'assurer que les droits d'accès aux réseaux/systèmes de TI et à l'information de l'Agence concordent avec les fonctions assignées;
- signaler immédiatement au personnel désigné de la Division de la sécurité de l'information tout usage abusif de l'information ou tout manquement à la présente directive.

# 7. CONFORMITÉ ET RAPPORTS

L'ASFC est responsable de s'assurer que ses programmes et services sont bien gérés. La Division de la sécurité du personnel et des normes professionnelles et la Division de la sécurité et de la continuité des TI doivent surveiller activement les pratiques de gestion et les contrôles liés à la présente directive. S'il y a des lacunes importantes ou que des améliorations sont nécessaires, les hauts fonctionnaires de l'Agence en seront informés.

Les employés produiront des rapports d'incident touchant la sécurité conformément aux exigences énoncées dans le Volume de sécurité de l'ASFC – Norme de sécurité matérielle pour le signalement des incidents de sécurité.

# 8. CONSÉQUENCES

L'ASM est responsable d'enquêter et d'intervenir en cas de signalement de non-conformité avec la présente directive et de s'assurer que des mesures correctives appropriées sont prises, au besoin. Tout employé reconnu coupable d'avoir enfreint les politiques, les directives ou les normes peut à juste titre faire l'objet d'une enquête de sécurité ainsi que de mesures disciplinaires pouvant aller jusqu'à la cessation d'emploi.

## 8.1. Examen de la directive

Le coordonnateur de la sécurité des TI (directeur, DSI) devrait procéder à un examen de la présente directive au moins tous les trois ans, ou avant, au besoin.

# 9. DOCUMENTS DE RÉFÉRENCE

**Secrétariat du Conseil du Trésor (SCT)**

- *Politique sur la sécurité du gouvernement*
- Ligne directrice sur la définition des exigences en matière d'authentification – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26262&section=text







- Norme sur l'assurance de l'identité et des justificatifs – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776&section=text
- Directive sur la gestion de l'identité – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16577&section=text
- Solutions technologiques d'authentification électronique – Architecture et spécifications de l'interface – Version 2.0 https://kantarainitiative.org/confluence/download/attachments/45059378/CA%20-%20CATS%20IAS%20V2.0_Deployment%20Profile_Final%20r7.2_fr.pdf?api=v2

**Centre de la sécurité des télécommunications du Canada (CSTC)**

- Directives en matière de sécurité des TI : Guide sur l'authentification des utilisateurs pour les systèmes TI – http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-fra.html

# 10. DEMANDES DE RENSEIGNEMENTS

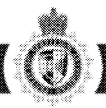
Les demandes de renseignements concernant la présente directive doivent être envoyées à l'adresse suivante :

| Bureau responsable | Coordonnées |
|---|---|
| **Direction générale de l'information, des sciences et de la technologie**<br>Division de la sécurité et de la continuité des opérations des TI | **Courriel** : CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca<br>**Intranet** : Sécurité TI |
| **Direction générale du contrôle**<br>Direction de la sécurité et des normes professionnelles | **Courriel** : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca |

# 11. DÉFINITIONS

Des définitions précises provenant de sources qui font autorité se trouvent dans le Lexique de la terminologie en sécurité.

Canada Border Services Agency | Agence des services frontaliers du Canada






# CBSA Security Controls Standard for Access Control for Information Systems

21 June 2016

PROTECTION • SERVICE • INTEGRITY



**Table of Contents**

# 1 Effective Date

This standard is effective July 1st, 2016.

# 2 Context

The Treasury Board Secretariat Directive on Departmental Security Management mandates the identification of security threats, risks and vulnerabilities to determine an appropriate set of security controls. Security controls must efficiently and effectively meet departmental security requirements.

The definition of domain security control profiles facilitates this process.

CBSA leverages the IT Security Risk Management: A Lifecycle Approach (ITSG-33) from Communications Security Establishment Canada (CSEC). ITSG-33 defines baseline security controls at the Protected B (medium integrity / medium availability) and Classified Secret (medium integrity / medium availability) levels. This standard focuses on the Access Control (AC) family of security controls.

| Classes | Technical Security Controls | Operational Security Controls | Management Security Controls |
|---|---|---|---|
| Families | AC – Access Control | AT – Awareness & Training | CA – Security Assessment & Authorization |
| | AU – Audit & Accountability | CM – Configuration Management | PL – Planning |
| | IA – Identification & Authentication | CP – Contingency Planning | RA – Risk Assessment |
| | SC – Systems & Communications Protection | IR – Incident Response | SA – System & Services Acquisition |
| | | MA – Maintenance | |

# 3 Application

This security controls standard applies to all individuals responsible for the selection, development, implementation and maintenance of CBSA electronic resources that is comprised of IT networks, systems, applications and data. These individuals include the program and service delivery managers (owners of systems and applications) and all technical personnel, and service providers (responsible for systems and applications development and maintenance).

Where the CBSA electronically shares information or is interconnected with external organizations, the CBSA will collaboratively engage its partners, clients and key stakeholders in the application of this standard.

Any project planning of a new information system or major changes to a legacy information system must adhere to this standard.

Managers of service provider contracts (e.g. external vendors, Shared Services Canada) must also ensure that service providers meet the requirements of this standard.

# 4 Standard Statement

This standard supports the CBSA Directive for Access Control in Information Systems.

## 4.1 Objective

The objective of this standard is to provide clear, concise, guidance with respect to the security controls of access that support the ability to permit or deny user access to resources within the information system.

## 4.2 Expected Results

The expected results of this standard are:

- Alignment of business domains, the threat environment and their security classification;
- Alignment of security controls with operational requirements to ensure optimal service delivery;
- Definition of an enterprise architecture that includes IT security requirements; and
- Defined baselines of security controls for information systems that the CBSA deems acceptable to support the domain's business activities.

# 5 Requirements

The table in Appendix A presents the minimum security controls required, by security control domain, for the design, implementation and on-going operations of CBSA information systems.

# 6 Compliance and Reporting

The CBSA Departmental Security Officer (DSO), the IT Security Coordinator, security practitioners and managers are responsible for monitoring compliance with this standard within CBSA, and for measuring the effectiveness of audit trails management.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Volume, Security Incident Reporting.

# 7 Consequences

The DSO is responsible for investigating and responding to reports of non-compliance with this standard and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies, directives or standards may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment.

# 8 Standard Review

This standard shall be reviewed at a minimum of every three years, or earlier, or as required by the IT Security Coordinator (ITSC) and the DSO.

# 9 Definitions

| Term | Definition |
|---|---|
| Information System | An information system is generally composed of data, computing platforms, communications networks, business applications, people, and processes, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. |
| Security Control | An administrative, operational, technical, physical or legal measure for managing security risk. This term is synonymous with safeguard. |
| Security Control Profile | A set of security controls established as the minimum mandatory requirements for a specific business domain and the associated information systems. A profile must satisfy TBS baseline security controls and CBSA business needs for security with due consideration for the CBSA threat context and technical context. |

# 10 References

## 10.1 CBSA

- Directive for Access Control in Information Systems

## 10.2 Treasury Board Secretariat

- Policy on Government Security
- Policy Framework for Information and Technology
- Policy on Access to Information
- Policy on Internal Audit
- Policy on Management of Information Technology
- Policy on Privacy Protection
- Directive on Recordkeeping
- Operational Security Standard: Management of IT Security (MITS)

## 10.3 Communications Security Establishment Canada

- CSEC – ITSG 33: IT Security Risk Management

## 11 Enquiries

Advice on this Standard can be obtained from:

IT Security & Continuity Division

Enterprise Services Directorate

Information Science and Technology Branch

CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca

and/or

Information & Infrastructure Security Division

Security and Professional Standards Directorate

Comptrollership Branch

Information_Security-Securite_de_linformation@cbsa-asfc.gc.ca

# Appendix A – Security Control Domains

This Appendix lists the required security controls.

## CBSA tailored – Protected B (Medium Integrity / Medium Availability) - Baseline

| Security Control Code | Security Control Name | Security Control Definition | Requirements |
|---|---|---|---|
| AC-01A | ACCESS CONTROL POLICY AND PROCEDURES- PART A | (A) The organization develops, documents, and disseminates to all staff:<br>(a) Directive on identity management and access control that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>(b) Procedures to facilitate the implementation of the directive on identity management and access control and associated access controls. | The following Enterprise Components demonstrates compliance with AC-01A security control:<br><br>• Policy on Information Security (POL-Policy on Information Security)<br>• Directive for Access Control in Information Systems (POL-Directive for Access Control in Information Systems)<br>• Policy on Information Technology (IT) Security (POL-Policy on Information Technology (IT) Security) |
| AC-01B | ACCESS CONTROL POLICY AND PROCEDURES- PART B | (B) The organization reviews and updates the current:<br>(a) Directive on identity management and access control at least every 3 years; and<br>(b) Access control procedures at least every year. | The following Enterprise Components demonstrates compliance with AC-01B security control :<br><br>• Security Policy and Program Coordination (PROG-SPPC)<br>• Policy on Information Security (POL-Policy on Information Security)<br>• Directive for Access Control in Information Systems (POL-Directive for Access Control in Information Systems)<br>• Policy on Information Technology (IT) Security (POL-Policy on Information Technology (IT) Security) |
| AC-02A | ACCOUNT MANAGEMENT - PART A | (A) The organization identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. | Information system must demonstrate compliance with AC-02A security control. |
| AC-02B | ACCOUNT MANAGEMENT - PART B | (B) The organization assigns account managers for information system accounts. | The following Enterprise Components demonstrates compliance with AC-02B security control:<br><br>• CRA National Helpdesk (CRA-NHD)<br>• ESD End User Computing Service (ESD-EUCS)<br>• Service Desk Services (ESD) (ESD-SERV DESK) |

| | | | |
|---|---|---|---|
| AC-02C | ACCOUNT MANAGEMENT - PART C | (C) The organization establishes conditions for group and role membership. | Information system must demonstrate compliance with AC-02C security control. |
| AC-02D | ACCOUNT MANAGEMENT - PART D | (D) The organization specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. | Information system must demonstrate compliance with AC-02D security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS)<br>• Managed Linux/Unix Platform Services (PaaS) (SSC-Unix/Linux-PaaS) |
| AC-02E | ACCOUNT MANAGEMENT - PART E | (E) The organization requires approvals by the information system authorizer, or their delegate, for requests to create information system accounts. | The following Enterprise Components demonstrates compliance with AC-02E security control:<br><br>• CRA National Helpdesk (CRA-NHD)<br>• ESD End User Computing Service (ESD-EUCS)<br>• Service Desk Services (ESD) (ESD-SERV DESK) |
| AC-02F | ACCOUNT MANAGEMENT - PART F | (F) The organization creates, enables, modifies, disables, and removes information system accounts in accordance with CBSA procedures or conditions. | The following Enterprise Components demonstrates compliance with AC-02F security control :<br><br>• CRA National Helpdesk (CRA-NHD)<br>• ESD End User Computing Service (ESD-EUCS)<br>• Service Desk Services (ESD) (ESD-SERV DESK) |
| AC-02G | ACCOUNT MANAGEMENT - PART G | (G) The organization monitors the use of information system accounts. | The following Enterprise Component demonstrates compliance with AC-02G security control:<br><br>• Information Security Program (PROG-INFOSEC) |
| AC-02H | ACCOUNT MANAGEMENT - PART H | (H) The organization notifies account managers:<br>(a) When accounts are no longer required;<br>(b) When users are terminated or transferred; and<br>(c) When individual information system usage or need-to-know changes. | The following Enterprise Component demonstrates compliance with AC-02H security control:<br><br>• Directive for Access Control in Information Systems (POL-Directive for Access Control in Information Systems) |

| | | | |
|---|---|---|---|
| AC-02I | ACCOUNT MANAGEMENT - PART I | (I) The organization authorizes access to the information system based on:<br>(a) A valid access authorization;<br>(b) Intended system usage; and<br>(c) Other attributes as required by the organization or associated missions/business functions. | The following Enterprise Components demonstrates compliance with AC-02I security control:<br><br>• CRA National Helpdesk (CRA-NHD)<br>• ESD End User Computing Service (ESD-EUCS)<br>• Service Desk Services (ESD) (ESD-SERV DESK) |
| AC-02_(07) | ACCOUNT MANAGEMENT \| ROLE-BASED SCHEMES | (a) The organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;<br>(b) The organization monitors privileged role assignments; and<br>(c) The organization takes actions when privileged role assignments are no longer appropriate. | Information system must demonstrate compliance with AC-02_(07) security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS)<br>• Managed Linux/Unix Platform Services (PaaS) (SSC-Unix/Linux-PaaS) |
| AC-03A | ACCESS ENFORCEMENT - PART A | (A) The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | Information system must demonstrate compliance with AC-03A security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS)<br>• Managed Linux/Unix Platform Services (PaaS) (SSC-Unix/Linux-PaaS) |
| AC-05A | SEPARATION OF DUTIES - PART A | (A) The organization:<br>(a) Separates duties of individuals;<br>(b) Documents separation of duties of individuals; and<br>(c) Defines information system access authorizations to support separation of duties. | Information system must demonstrate compliance with AC-05A security control. |
| AC-06A | LEAST PRIVILEGE - PART A | (A) The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | Information system must demonstrate compliance with AC-06A security control. |
| AC-06_(02) | LEAST PRIVILEGE \| NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS | The organization requires that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions. | The following Enterprise Component demonstrates compliance with AC-06_(02) security control:<br><br>• Privilege User Risk Management (PROG-PURM) |

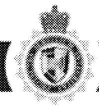
| | | | |
|---|---|---|---|
| AC-06_(05) | LEAST PRIVILEGE \| PRIVILEGED ACCOUNTS | The organization restricts privileged accounts on the information system to specifically authorized personnel. | The following Enterprise Component demonstrates compliance with AC-06_(05) security control:<br><br>• Privilege User Risk Management (PROG-PURM) |
| AC-06_(10) | LEAST PRIVILEGE \| PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. | Information system must demonstrate compliance with AC-06_(10) security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS)<br>• Managed Linux/Unix Platform Services (PaaS) (SSC-Unix/Linux-PaaS) |
| AC-07A | UNSUCCESSFUL LOGIN ATTEMPTS - PART A | (A) The information system enforces a limit of 3 consecutive invalid logon attempts by a user during a period of 15 minutes. | Information system must demonstrate compliance with AC-07A security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS)<br>• Managed Linux/Unix Platform Services (PaaS) (SSC-Unix/Linux-PaaS) |
| AC-07B | UNSUCCESSFUL LOGIN ATTEMPTS - PART B | (B) The information system automatically locks the account/node for 30 minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded. | Information system must demonstrate compliance with AC-07B security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS)<br>• Managed Linux/Unix Platform Services (PaaS) (SSC-Unix/Linux-PaaS) |

| | | | |
|---|---|---|---|
| AC-08A | SYSTEM USE NOTIFICATION - PART A | (A) The information system displays to users a system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on the Use of Electronic Networks. | Information system must demonstrate compliance with AC-08A security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS) |
| AC-08B | SYSTEM USE NOTIFICATION - PART B | (B) The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system. | Information system must demonstrate compliance with AC-08B security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS) |
| AC-11B | SESSION LOCK - PART B | (B) The information system retains the session lock until the user re-establishes access using established identification and authentication procedures. | Information system must demonstrate compliance with AC-11B security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS) |
| AC-11_(01) | SESSION LOCK \| PATTERN-HIDING DISPLAYS | The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. | Information system must demonstrate compliance with AC-11_(01) security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS) |
| AC-14A | PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION - PART A | (A) The organization identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions. | Information system must demonstrate compliance with AC-14A security control. |
| AC-16_(05) | SECURITY ATTRIBUTES \| ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES | The information system displays security attributes in human-readable form on each object that the system transmits to output devices to identify special dissemination, handling, or distribution instructions using human-readable standard naming conventions. | Information system must demonstrate compliance with AC-16_(05) security control. |

| | | | |
|---|---|---|---|
| AC-17A | REMOTE ACCESS - PART A | (A) The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. | Information system must demonstrate compliance with AC-17A security control. This can be achieved by leveraging the following Common Component:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS) |
| AC-17B | REMOTE ACCESS - PART B | (B) The organization authorizes remote access to the information system prior to allowing such connections. | Information system must demonstrate compliance with AC-17B security control. This can be achieved by leveraging the following Common Component:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS) |
| AC-17_(01) | REMOTE ACCESS \| AUTOMATED MONITORING / CONTROL | The information system monitors and controls remote access methods. | Information system must demonstrate compliance with AC-17_(01) security control. This can be achieved by leveraging the following Common Components:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS)<br>• Managed Mainframe z/OS Platform Service (PaaS) (SSC-MF-PaaS)<br>• SSC Infrastructure Security Services (SSC-IS)<br>• Managed Linux/Unix Platform Services (PaaS) (SSC-Unix/Linux-PaaS) |
| AC-17_(02) | REMOTE ACCESS \| PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. The cryptography must be compliant with the requirements of SC-13. | Information system must demonstrate compliance with AC-17_(02) security control. This can be achieved by leveraging the following Common Component:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS) |
| AC-17_(03) | REMOTE ACCESS \| MANAGED ACCESS CONTROL POINTS | The information system routes all remote accesses through managed network access control points. | Information system must demonstrate compliance with AC-17_(03) security control. This can be achieved by leveraging the following Common Component:<br><br>• Managed Windows Server Platform Services (PaaS) (SSC-Win-PaaS) |
| AC-17_AA | REMOTE ACCESS - PART AA | (AA) The organization ensures that all employees working off site safeguard information as per the minimum requirements in accordance with the TBS Operational Security Standard on Physical Security [Reference 6]. | The following Enterprise Component demonstrates compliance with AC-17_AA security control:<br><br>• Physical Security Program (PROG-PHYSEC) |

| | | | |
|---|---|---|---|
| AC-18A | WIRELESS ACCESS-PART A | (A) The organization establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access. | The following Enterprise Component demonstrates compliance with AC-18A security control:<br><br>• Directive on the Use of Wireless Technology (POL-Directive on the Use of Wireless Technology ) |
| AC-20A | USE OF EXTERNAL INFORMATION SYSTEMS - PART A | (A) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems. | The following Enterprise Components demonstrates compliance with AC-20A security control:<br><br>• ESD Data Centre Compute Service (ESD-DCCS)<br>• ESD Network Service (ESD-NS)<br>• Service Provider Management Services (ESD-PROVIDER MNGT) |
| AC-20B | USE OF EXTERNAL INFORMATION SYSTEMS - PART B | (B) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, or transmit organization-controlled information using external information systems. | The following Enterprise Components demonstrates compliance with AC-20B security control:<br><br>• ESD Data Centre Compute Service (ESD-DCCS)<br>• ESD Network Service (ESD-NS)<br>• Service Provider Management Services (ESD-PROVIDER MNGT) |
| AC-20_(02) | USE OF EXTERNAL INFORMATION SYSTEMS \| PORTABLE STORAGE DEVICES | The organization prohibits the use of organization-controlled mobile devices by authorized individuals on external information systems. | The following Enterprise Component demonstrates compliance with AC-20_(02) security control:<br><br>• Policy on the Use of Electronic Resources (POL-Policy on the Use of Electronic Resources ) |
| AC-20_(03) | USE OF EXTERNAL INFORMATION SYSTEMS \| NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES | The organization prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information. | The following Enterprise Component demonstrates compliance with AC-20_(03) security control:<br><br>• Policy on the Use of Electronic Resources (POL-Policy on the Use of Electronic Resources ) |
| AC-20_(04) | USE OF EXTERNAL INFORMATION SYSTEMS \| NETWORK ACCESSIBLE STORAGE DEVICES | The organization prohibits the use of network accessible storage devices in external information systems. | The following Enterprise Component demonstrates compliance with AC-20_(04) security control:<br><br>• Policy on the Use of Electronic Resources (POL-Policy on the Use of Electronic Resources ) |
| AC-21_(100) | USER-BASED COLLABORATION AND INFORMATION SHARING | The organization ensures, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations. | Information system must demonstrate compliance with AC-21_(100) security control. |

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme de l'ASFC en matière de contrôles de sécurité pour le contrôle d'accès des systèmes d'information




Le 21 Juin 2016

PROTECTION • SERVICE • INTÉGRITÉ



**Table des Matières**

# 1 Date d'entrée en vigueur

La présente norme entre en vigueur au 1er Juillet 2016.

# 2 Contexte

La *Directive sur la gestion de la sécurité ministérielle* du Secrétariat du Conseil du Trésor exige qu'on définisse les menaces à la sécurité, les risques et les vulnérabilités afin de fixer un ensemble approprié de contrôles de sécurité qui remplissent de manière efficace et efficiente les exigences de l'ASFC en matière de sécurité.

Ce processus est facilité par la définition des profils de contrôle de sécurité de domaine.

L'ASFC s'appuie sur *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33), un document émanant du Centre de la sécurité des télécommunications Canada (CSTC). Le guide ITSG-33 énonce les contrôles de sécurité de base pour les niveaux Protégé B (intégrité moyenne/disponibilité moyenne) et Secret (intégrité moyenne/disponibilité moyenne). Le présent document met l'accent sur la norme pour la famille de contrôles d'accès (AC) qui fait partie des contrôles de sécurité.

| Classes | Contrôles de sécurité techniques | Contrôles de sécurité opérationnels | Contrôles de sécurité de gestion |
|---|---|---|---|
| Familles | AC – Contrôle d'accès | AT – Formation et sensibilisation | CA – Évaluation et autorisation de sécurité |
| | AU – Vérification et responsabilisation | GC – Gestion des configurations | PL – Planification |
| | IA – Identification et authentification | CP – Planification d'urgence | RA – Évaluation des risques |
| | SC – Protection des systèmes et des communications | IR – Intervention en cas d'incident | SA – Acquisition des systèmes et des services |
| | | MA – Maintenance | |

# 3 Application

La présente norme de contrôles de sécurité s'applique à toutes les personnes responsables de la sélection, de l'élaboration, de la mise en œuvre et du maintien des ressources électroniques de l'ASFC des services frontaliers du Canada (ASFC), à savoir les réseaux, les systèmes, les applications et les données de technologie de l'information (TI). Ces personnes comprennent les gestionnaires d'exécution des programmes et de prestation des services (responsables des systèmes et des applications), tout le personnel technique, les employés et le fournisseur de services (ressources techniques chargées de l'élaboration et du maintien des systèmes et des applications).

Dans les cas où l'ASFC communique des renseignements de façon électronique ou est interconnectée à des organisations externes, l'ASFC collabore avec ses partenaires, ses clients et les intervenants clés en vue d'appliquer cette norme.

Tout projet prévoyant un nouveau système d'information ou des changements importants à un ancien système d'information doit respecter cette norme.

Les gestionnaires des marchés conclus avec les fournisseurs de services (p. ex. les fournisseurs externes et Services partagés Canada) doivent également s'assurer que les fournisseurs de services satisfont aux exigences de la norme.

Dans les cas où l'ASFC communique des renseignements de façon électronique ou est interconnectée à des organisations externes, l'ASFC collabore avec ses partenaires, ses clients et les intervenants clés en vue d'appliquer cette norme en fonction de leur relation de travail mutuelle.

Tout projet prévoyant un nouveau système d'information ou des changements importants à un ancien système d'information doit respecter cette norme.

Les gestionnaires des marchés conclus avec les fournisseurs de service (p. ex., les fournisseurs externes et Services partagés Canada [SPC]) doivent également s'assurer que les fournisseurs de service satisfont aux exigences de la norme.

# 4 Énoncé de la norme

La présente norme soutient la Directive sur le contrôle de l'accès aux systèmes d'information de l'ASFC.

## 4.1 Objectif

La présente norme a pour objectif de fournir une orientation claire et concise en ce qui a trait aux contrôles de sécurité relatifs à l'accès, c'est-à-dire les contrôles qui permettent de déterminer si un utilisateur peut accéder ou non aux ressources du système d'information.

## 4.2 Résultats prévus

La présente norme vise l'obtention des résultats suivants :

- L'harmonisation des domaines d'activités et de leur classification de sécurité et de l'environnement de menace.
- L'harmonisation des contrôles de sécurité avec les impératifs opérationnels pour assurer une livraison optimale des services.
- La définition d'une architecture organisationnelle assortie d'exigences en matière de sécurité des TI.
- La définition de contrôles de sécurité de base pour les systèmes d'information qui sont satisfaisants, selon l'ASFC, pour soutenir les activités opérationnelles du domaine.

## 5 Exigences

Le tableau qui figure à l'annexe A présente les exigences minimales en matière de contrôles de sécurité, réparties par le domaine de contrôle de sécurité, requises pour appuyer l'élaboration, la mise en œuvre et l'exploitation continue des systèmes d'information de l'ASFC.

## 6 Conformité et établissement de rapports

L'ASM, le Coordinateur de la Sécurité des TI, les praticiens de la sécurité et les gestionnaires sont responsables pour la surveillance de la conformité avec cette norme dans l'ASFC, et pour mesurer l'efficacité de la gestion des dossiers de vérification.

Les employés doivent rapporter les incidents de sécurité conformément aux procédures détaillées dans le Volume de Sécurité de l'ASFC, Rapport des incidents de sécurité.

## 7 Conséquences

L'ASM doit enquêter et intervenir lorsque des cas de non-conformité avec la norme sont signalés et voir à ce que les mesures correctives appropriées soient prises au moment opportun, s'il y a lieu. Tout membre du personnel qui enfreint les politiques, les directives ou les normes peut faire l'objet d'un examen qui pourrait entraîner la révocation de sa côte de fiabilité de l'ASFC ainsi que de mesures disciplinaires pouvant aller jusqu'au renvoi.

## 8 Examen de la norme

La norme fera l'objet d'un examen au moins tous les trois ans, ou lorsque le CSTI et l'ASM l'exigent.

## 9 Définitions

| Termes | Définition |
|---|---|
| Système d'information | Un système d'information est généralement composé de données, de plates-formes informatiques, de réseaux de communications, d'applications administratives, de personnes et de processus organisés pour permettre la collecte, le traitement, la maintenance, l'utilisation, le partage, la diffusion ou l'élimination d'information. |

| Termes | Définition |
|---|---|
| Contrôle de sécurité | Une mesure administrative, opérationnelle, technique, physique ou juridique pour gérer les risques liés à la sécurité. Ce terme est synonyme de mesure de protection. |
| Profil de contrôle de sécurité | Un ensemble de contrôles de sécurité qu'on établit comme exigences minimales obligatoires pour un domaine d'activité donné et les systèmes d'information connexes. Un profil doit répondre aux besoins opérationnels de l'ASFC et aux contrôles de sécurité de référence du Conseil du Trésor, tout en tenant compte du contexte technique et du contexte de menace de l'organisation. |

# 10 Références

## 10.1 ASFC

- Directive sur le contrôle de l'accès aux systèmes d'information

## 10.2 Secrétariat du Conseil du Trésor

- Politique sur la sécurité du gouvernement
- Cadre stratégique pour l'information et la technologie
- Politique sur l'accès à l'information
- Politique sur la vérification interne
- Politique sur la gestion des technologies de l'information
- Politique sur la protection de la vie privée
- Directive sur la tenue de documents
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)

## 10.3 Centre de la sécurité des télécommunications Canada

- ITSG-33 du CSTC : Gestion des risques relatifs à la sécurité de la TI

# 11 Demandes de renseignements

Pour obtenir des conseils au sujet de la présente norme, communiquer avec :

Division de la sécurité et de la continuité des opérations de la TI

Direction des services organisationnels

Direction générale de l'information, des sciences et de la technologie

CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca

Ou

Division de l'infrastructure et de la sécurité de l'information

Direction de la sécurité et des normes professionnelles

Direction générale du contrôle

Information_Security-Securite_de_linformation@cbsa-asfc.gc.ca

## Annexe A – Domaines des contrôles de sécurité

La liste suivante présente les contrôles de sécurité requis.

### Exigences de base (Protégé B / Intégrité Moyenne Disponibilité Moyenne)

| Numéro du contrôle de sécurité | Nom du contrôle de sécurité | Définition du contrôle de sécurité | Exigences |
|---|---|---|---|
| AC-01A | POLITIQUE ET PROCÉDURES DE CONTRÔLE D'ACCÈS — PARTIE A | (A) L'organisation élabore et consigne ce qui suit et les diffuse à tout le personnel :<br>(a) une directive sur la gestion de l'identité et le contrôle d'accès qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect ; et<br>(b) des procédures pour faciliter la mise en œuvre de la directive sur la gestion de l'identité et le contrôle d'accès et des contrôles d'accès connexes. | Les composants suivants de l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-01A :<br><br>• Politique sur la sécurité de l'information (POL-Politique sur la sécurité de l'information)<br>• Directive sur le contrôle d'accès aux systèmes d'information (POL-Directive sur le contrôle d'accès aux systèmes d'information)<br>• Politique sur la sécurité des technologies de l'information (TI) (POL-Politique sur la sécurité des technologies de l'information (TI)) |
| AC-01B | POLITIQUE ET PROCÉDURES DE CONTRÔLE D'ACCÈS — PARTIE B | (B) L'organisation examine et met à jour :<br>(a) la directive sur la gestion de l'identité et le contrôle d'accès au moins tous les trois ans ; et<br>(b) les procédures de contrôle d'accès au moins tous les ans. | Les composants suivants de l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-01B :<br><br>• Politique sur la sécurité et coordination du programme (PROG-SPPC)<br>• Politique sur la sécurité de l'information (POL-Politique sur la sécurité de l'information)<br>• Directive sur le contrôle d'accès aux systèmes d'information (POL-Directive sur le contrôle d'accès aux systèmes d'information)<br>• Politique sur la sécurité des technologies de l'information (TI) (POL-Politique sur la sécurité des technologies de l'information (TI)) |
| AC-02A | GESTION DES COMPTES — PARTIE A | (A) L'organisation établit et sélectionne les types de compte de système d'information suivants pour appuyer les fonctions opérationnelles et les missions : les comptes individuels; les comptes partagés; les comptes de groupe; les comptes système; les comptes anonymes ou d'invité; les comptes d'urgence; les comptes de développeur; de fabricant ou de fournisseur; et les comptes temporaires, ainsi que les comptes de service. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-02A. |
| AC-02B | GESTION DES COMPTES — PARTIE B | (B) L'organisation nomme des gestionnaires de compte pour les comptes de système d'information. | Les composants suivants de l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-02B :<br><br>• Bureau d'aide national de l'ARC |

| | | | |
|---|---|---|---|
| | | | (BAN-ARC)<br>• Service de soutien informatique à l'intention des utilisateurs finaux (service électronique) (ESD-EUCS)<br>• Services du bureau d'aide (services électroniques) (ESD-SERV DESK) |
| AC-02C | GESTION DES COMPTES — PARTIE C | (C) L'organisation établit les conditions en fonction du groupe et du rôle. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-02C. |
| AC-02D | GESTION DES COMPTES — PARTIE D | (D) L'organisation précise les utilisateurs autorisés du système d'information, les groupes et les rôles, ainsi que les autorisations d'accès (c.-à-d. les droits d'accès) et d'autres attributs (au besoin) pour chaque compte. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-02D. Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS)<br>• Plateforme-service gérée (PaaS) — Linux/Unis (SSC-Unix/Linux-PaaS) |
| AC-02E | GESTION DES COMPTES — PARTIE E | (E) L'organisation doit obtenir l'approbation de l'autorisateur du système d'information ou de la personne déléguée pour les demandes de création de comptes de système d'information. | Les composants suivants de l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-02E :<br><br>• Bureau d'aide national de l'ARC (BAN-ARC)<br>• Service de soutien informatique à l'intention des utilisateurs finaux (service électronique) (ESD-EUCS)<br>• Services du bureau d'aide (services électroniques) (ESD-SERV DESK) |
| AC-02F | GESTION DES COMPTES — PARTIE F | (F) L'organisation crée, active, modifie, désactive et retire les comptes de système d'information conformément aux conditions et aux procédures définies par l'ASFC. | Les composants suivants de l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-02F :<br><br>• Bureau d'aide national de l'ARC (BAN-ARC)<br>• Service de soutien informatique à l'intention des utilisateurs finaux (service électronique) (ESD-EUCS)<br>• Services du bureau d'aide (services électroniques) (ESD-SERV DESK) |
| AC-02G | GESTION DES COMPTES — PARTIE G | (G) L'organisation surveille l'utilisation des comptes de système d'information. | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-02G :<br><br>• Programme de sécurité de l'information (PROG-INFOSEC) |
| AC-02H | GESTION DES COMPTES — PARTIE H | (H) L'organisation informe les gestionnaires de compte :<br>(a) lorsque les comptes ne sont plus requis ;<br>(b) lorsque les utilisateurs quittent leur poste ou sont mutés ; et<br>(c) lorsque l'utilisation du système d'information ou le besoin de connaître d'un | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-02H :<br><br>• Directive sur le contrôle d'accès aux systèmes d'information (POL- |

| | | | |
|---|---|---|---|
| | | utilisateur change. | Directive sur le contrôle d'accès aux systèmes d'information) |
| AC-02I | GESTION DES COMPTES — PARTIE I | (I) L'organisation autorise l'accès au système d'information selon :<br>(a) une autorisation d'accès valide ;<br>(b) l'utilisation prévue du système ;<br>(c) d'autres attributs exigés par l'organisation ou des missions ou fonctions opérationnelles connexes. | Les composants suivants de l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-02I :<br><br>• Bureau d'aide national de l'ARC (BAN-ARC)<br>• Service de soutien informatique à l'intention des utilisateurs finaux (service électronique) (ESD-EUCS)<br>• Services du bureau d'aide (services électroniques) (ESD-SERV DESK) |
| AC-02_(07) | GESTION DES COMPTES \| PLANS BASÉS SUR LES RÔLES | (a) L'organisation établit et administre les comptes utilisateur privilégiés conformément à un plan de contrôle d'accès basé sur les rôles qui regroupe l'accès et les droits d'accès au système d'information permis par rôle.<br>(b) L'organisation surveille les attributions de rôles privilégiés.<br>(c) L'organisation prend des mesures lorsque les attributions de rôles privilégiés ne conviennent plus. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-02_(07). Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS)<br>• Plateforme-service gérée (PaaS) — Linux/Unis (SSC-Unix/Linux-PaaS) |
| AC-03A | APPLICATION DE L'ACCÈS — PARTIE A | (A) Le système d'information applique les autorisations approuvées pour l'accès logique aux ressources du système et à l'information conformément aux politiques de contrôle d'accès applicables. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-03A. Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS)<br>• Plateforme-service gérée (PaaS) — Linux/Unis (SSC-Unix/Linux-PaaS) |
| AC-05A | SÉPARATION DES TÂCHES — PARTIE A | (A) L'organisation :<br>(a) sépare les tâches des personnes ;<br>(b) consigne la séparation des tâches des personnes ; et<br>(c) définit les autorisations d'accès au système d'information pour appuyer la séparation des tâches. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-05A. |
| AC-06A | DROIT D'ACCÈS MINIMAL — PARTIE A | (A) L'organisation utilise le principe du droit d'accès minimal, ce qui autorise l'accès uniquement aux utilisateurs (ou aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées conformément aux missions et aux fonctions opérationnelles de l'organisation. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-06A. |
| AC-06_(02) | DROIT D'ACCÈS MINIMAL \| ACCÈS NON PRIVILÉGIÉ POUR LES FONCTIONS NON LIÉES À LA SÉCURITÉ | L'organisation exige des utilisateurs de comptes ou de rôles de système d'information qui ont accès aux fonctions de sécurité et à l'information sur la sécurité qu'ils utilisent des comptes ou des rôles non privilégiés pour accéder à des fonctions qui | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-06_(02) :<br><br>• Gestion du risque des utilisateurs |

| | | | |
|---|---|---|---|
| | | ne sont pas liées à la sécurité. | privilégiés (PROG-PURM) |
| AC-06_(05) | DROIT D'ACCÈS MINIMAL \| COMPTES PRIVILÉGIÉS | L'organisation restreint les comptes privilégiés sur le système d'information au personnel autorisé. | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-06_(05) :<br><br>• Gestion du risque des utilisateurs privilégiés(PROG-PURM) |
| AC-06_(10) | DROIT D'ACCÈS MINIMAL \| INTERDICTION AUX UTILISATEURS NON PRIVILÉGIÉS D'EXÉCUTER DES FONCTIONS PRIVILÉGIÉES | Le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, y compris la désactivation, le contournement ou la modification des mesures de protection et contremesures de sécurité mises en œuvre. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-06_(10). Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS)<br>• Plateforme-service gérée (PaaS) — Linux/Unis (SSC-Unix/Linux-PaaS) |
| AC-07A | TENTATIVES D'OUVERTURE DE SESSION INFRUCTUEUSES — PARTIE A | (A) Le système d'information applique une limite de 3 tentatives d'ouverture de session invalides consécutives par utilisateur sur une période de 15 minutes. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-07A. Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS)<br>• Plateforme-service gérée (PaaS) — Linux/Unis (SSC-Unix/Linux-PaaS) |
| AC-07B | TENTATIVES D'OUVERTURE DE SESSION INFRUCTUEUSES — PARTIE B | (B) Le système d'information verrouille automatiquement le compte ou le nœud pendant 30 minutes ou jusqu'à ce qu'un administrateur le libère lorsque le nombre maximal de tentatives infructueuses est dépassé. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-07B. Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS)<br>• Plateforme-service gérée (PaaS) — Linux/Unis (SSC-Unix/Linux-PaaS) |
| AC-08A | AVIS D'UTILISATION SYSTÈME — PARTIE A | (A) Le système d'information, avant d'accorder l'accès, affiche aux utilisateurs un message ou une bannière d'avis d'utilisation du système, qui comprend des avis en matière de confidentialité et de sécurité conformément à la *Politique sur l'utilisation acceptable des dispositifs et des réseaux* du SCT. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-08A. Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS) |
| AC-08B | AVIS D'UTILISATION SYSTÈME — PARTIE B | (B) Le système d'information continue d'afficher le message ou la bannière d'avis jusqu'à ce que l'utilisateur accepte les | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-08B. Les composantes |

| | | | |
|---|---|---|---|
| | | modalités d'utilisation et prend des mesures précises en vue d'ouvrir une session ou d'accéder au système. | communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS) |
| AC-11B | VERROUILLAGE DE SESSION — PARTIE B | (B) Le système d'information maintient le verrouillage de la session jusqu'à ce que l'utilisateur rétablisse l'accès en exécutant les procédures établies d'identification et d'authentification. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-11B. Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS) |
| AC-11_(01) | VERROUILLAGE DE SESSION \| MASQUAGE DE L'AFFICHAGE AU MOYEN D'UNE IMAGE | Au moyen du verrouillage de session, le système d'information utilise une image visible afin de masquer l'information qui était visible auparavant sur l'affichage. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-11_(01). Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS) |
| AC-14A | OPÉRATIONS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION | (A) L'organisation recense les opérations que l'utilisateur peut exécuter dans le système d'information sans devoir s'identifier ou s'authentifier, conformément aux fonctions opérationnelles et aux missions de l'organisation. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-14A. |
| AC-16_(05) | ATTRIBUTS DE SÉCURITÉ \| AFFICHAGE D'ATTRIBUT POUR LES DISPOSITIFS DE SORTIE | Le système d'information affiche sous forme lisible les attributs de sécurité de chaque objet que le système transmet à des dispositifs de sortie afin de cerner les instructions spéciales de diffusion, de traitement ou de distribution conformément aux conventions d'appellation standard, en langage lisible par une personne. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-16_(05). |
| AC-17A | ACCÈS À DISTANCE — PARTIE A | (A) L'organisation définit et consigne les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre de chaque type d'accès à distance autorisé. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-17A. La composante commune suivante peut être utilisée à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS) |
| AC-17B | ACCÈS À DISTANCE — PARTIE B | (B) L'organisation autorise l'accès à distance au système d'information avant d'autoriser de telles connexions. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-17B. La composante commune suivante peut être utilisée à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS) |

| | | | |
|---|---|---|---|
| AC-17_(01) | ACCÈS À DISTANCE \| SURVEILLANCE ET CONTRÔLE AUTOMATISÉS | Le système d'information surveille et contrôle les méthodes d'accès à distance. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-17_(01). Les composantes communes suivantes peuvent être utilisées à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS)<br>• Plateforme-service gérée (PaaS) — Ordinateur central z/OS (SSC-MF-PaaS)<br>• SSC Infrastructure Security Services (SSC-IS)<br>• Plateforme-service gérée (PaaS) — Linux/Unis (SSC-Unix/Linux-PaaS) |
| AC-17_(02) | ACCÈS À DISTANCE \| PROTECTION DE LA CONFIDENTIALITÉ ET DE L'INTÉGRITÉ AU MOYEN DU CHIFFREMENT | Le système d'information met en œuvre des mécanismes cryptographiques pour protéger la confidentialité et l'intégrité des sessions d'accès à distance. La cryptographie doit être conforme aux exigences du contrôle SC-13. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-17_(02). La composante commune suivante peut être utilisée à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS) |
| AC-17_(03) | ACCÈS À DISTANCE \| POINTS DE CONTRÔLE D'ACCÈS GÉRÉS | Le système d'information achemine tous les accès à distance au moyen de points de contrôle d'accès réseau gérés. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-17_(03). La composante commune suivante peut être utilisée à cette fin :<br><br>• Plateforme-service gérée (PaaS) — Serveur Windows (SSC-Win-PaaS) |
| AC-17_AA | ACCÈS À DISTANCE — PARTIE AA | (AA) L'organisation s'assure que tous les employés qui travaillent à l'extérieur de ses locaux protègent l'information conformément aux exigences minimales précisées dans la *Norme opérationnelle sur la sécurité matérielle* du SCT [référence 6]. | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-17_AA :<br><br>• Programme de sécurité matérielle (PROG-PHYSEC) |
| AC-18A | ACCÈS SANS FIL — PARTIE A | (A) L'organisation établit les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre de l'accès sans fil. | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-18A :<br><br>• Directive sur l'utilisation de la technologie sans fil (POL-Directive sur l'utilisation de la technologie sans fil) |
| AC-20A | UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES — PARTIE A | (A) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent ou maintiennent des systèmes d'information externes, définit les modalités permettant aux personnes autorisées d'accéder au système d'information à partir de systèmes d'information externes. | Les composants suivants de l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-20A :<br><br>• Service de soutien informatique des centres de données (service électronique) (ESD-DCCS)<br>• Service de réseau (service électronique) (ESD-NS)<br>• Services de gestion des fournisseurs de services (ESD-PROVIDER MNGT) |
| AC-20B | UTILISATION DE | (B) L'organisation, conformément aux | Les composants suivants de |

| | | | |
|---|---|---|---|
| | SYSTÈMES D'INFORMATION EXTERNES — PARTIE B | relations de confiance établies avec d'autres organisations qui possèdent, exploitent ou maintiennent des systèmes d'information externes, définit les modalités permettant aux personnes autorisées de traiter, de stocker ou de transmettre de l'information contrôlée par l'organisation à l'aide de systèmes d'information externes. | l'architecture de l'organisation sont en conformité avec les exigences du contrôle de sécurité AC-20B :<br><br>• Service de soutien informatique des centres de données (service électronique) (ESD-DCCS)<br>• Service de réseau (service électronique) (ESD-NS)<br>• Services de gestion des fournisseurs de services (ESD-PROVIDER MNGT) |
| AC-20_(02) | UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES \| DISPOSITIFS DE STOCKAGE PORTATIFS | L'organisation interdit l'utilisation de dispositifs mobiles qu'elle contrôle par des personnes autorisées sur les systèmes d'information externes. | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-20_(02) :<br><br>• Politique sur l'utilisation des ressources électroniques (POL-Politique sur l'utilisation des ressources électroniques) |
| AC-20_(03) | UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES \| SYSTÈMES, COMPOSANTS ET DISPOSITIFS N'APPARTENANT PAS À L'ORGANISATION | L'organisation interdit l'utilisation de systèmes d'information, de composants système et de dispositifs ne lui appartenant pas, à des fins de traitement, de stockage ou de transmission d'information organisationnelle. | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-20_(03) :<br><br>• Politique sur l'utilisation des ressources électroniques (POL-Politique sur l'utilisation des ressources électroniques) |
| AC-20_(04) | UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES \| DISPOSITIFS DE STOCKAGE ACCESSIBLES PAR RÉSEAU | L'organisation interdit l'utilisation de dispositifs de stockage accessibles par réseau dans des systèmes d'information externes. | Le composant suivant de l'architecture de l'organisation est en conformité avec les exigences du contrôle de sécurité AC-20_(04) :<br><br>• Politique sur l'utilisation des ressources électroniques (POL-Politique sur l'utilisation des ressources électroniques) |
| AC-21_(100) | COLLABORATION ET ÉCHANGE D'INFORMATION ENTRE UTILISATEURS | L'organisation, suite à des ententes écrites, veille à prendre les mesures de protection appropriées de l'information de nature délicate échangée avec d'autres gouvernements et organisations. | Le système d'information doit être conforme aux exigences du contrôle de sécurité AC-21_(100). |

Canada Border Services Agency | Agence des services frontaliers du Canada



# Directive for Identity Management and Authentication in Information Systems

January 20, 2015

PROTECTION • SERVICE • INTEGRITY





## Contents







Canada Border Services Agency | Agence des services frontaliers du Canada



# 1. EFFECTIVE DATE

This directive is effective January 20st, 2015.

# 2. DIRECTIVE STATEMENT

## 2.1. Objective

Ensure effective information technology (IT) identity management practices are disseminated in the Canada Border Services Agency to protect Agency electronic services, critical systems, resources, and information.

It is also closely related to the Directive for Access Control in Information Systems.

## 2.2. Expected Results

The expected results of this directive are:

a) IT Identity management and authentication is an identifiable and integral element of Agency electronic services, critical systems, resources, and information;
b) That the Agency is dealing with known *entities* when delivering electronic services; and
c) Integrity of entity identity and authentication and the associated internal controls effectively mitigates unauthorized access, authority, disclosure, destruction, removal, modification and misuse.

# 3. APPLICATION

This directive applies to:

a) All entities accessing Agency electronic services, critical systems, resources, and information;
b) CBSA authorized managers with identity management responsibilities as outlined in this Directive.

# 4. CONTEXT

The Policy on Government Security (PGS) requires each organization to properly validate that the identity and credential of any individual or institution with whom it is transacting is legitimate.

CBSA must implement a common identity and authentication framework. Identity management practices are to reflect a government-wide approach which allows for interoperability and exchange of individuals' identity information, where appropriate, meeting the overall objectives of the Government of Canada and the respective mandates of departments.

This directive is intended to be read in concert with the associated CBSA Directive for Access Control in Information Systems.







# 5. REQUIREMENTS

a) All CBSA IT systems, applications and services must adhere to this Directive for Identity Management and Authentication in Information Systems;

b) Users are to be assigned a single unique user identification code (User ID) created in accordance with IT policy / standards, that will be used for accessing all Agency IT networks / systems, i.e. distributed environment, mainframe, etc.;

c) In exceptional circumstances and only when authorized by a Management Level 3 (ML3) or above, and in agreement with IT Security and Continuity Division (ITSCD), users may be granted multiple user IDs or continue to use a non-standard user ID, when absolutely required to perform work-related duties;

d) Users who require privileges when accessing CBSA systems are to be assigned a special account with a unique user identification code created in accordance with IT policy / standards;

e) Users must be security screened to the level appropriate to their duties;

f) Except for public web sites, all entities must be uniquely identified and authenticated before obtaining access to CBSA electronic services, resources and information;

g) Identification and authentication information is protected from unauthorized disclosure; and

h) Where required, mechanisms are implemented to provide identity and credential assurance for entities including individuals, organizations and devices.

# 6. ROLES & RESPONSIBILITIES

## 6.1. Chief Information Officer (CIO)

The CIO is responsible for:

- Ensuring that the identity management and authentication processes used by information systems are identified, reviewed and validated; and
- Designating an office responsible for coordinating identity authentication activities across the Agency.

## 6.2. Departmental Security Officer (DSO)

The DSO is responsible for:

- Organizing the review of this directive and coordinating updates as required;
- Assisting PSDMs with user identity and authentication advice and guidance as required;
- Providing user security clearance information to managers when requested;
- Providing security briefings to all users;
- Ensuring security certificates have been signed by the manager and the privileged user; and
- Ensuring IT identity management requirements in this directive and supporting standard(s) and guidelines are implemented Agency-wide.







## 6.3. IT Security Coordinator (ITSC)

The IT Security Coordinator is responsible for:

- Ensuring that any service provider delivers the system-level capability to support identification and authentication requirements defined in this Directive and associated standard(s); and
- Developing new policy instruments and updating existing ones related to IT Identity.

## 6.4. Program and Service Delivery Managers (PSDMs)

PSDMs are responsible for:

- Ensuring that all users, organizations and devices requiring access to CBSA electronic services, resources and information are identified and authenticated according to the requirements of this Directive and associated directives, standards(s) and guidelines.

## 6.5. External Service Providers (including SSC)

External Service Providers are responsible for:

- Adhering to this CBSA directive and associated standard(s) and not circumventing it as part of their duties when administering CBSA IT systems and applications.

## 6.6. Enterprise Architects

Enterprise Architects are responsible for:

- Maintaining an authoritative list of all identity credential solutions approved by CBSA[1]; and
- Providing subject matter expertise and technical consultation to PSDMs and their resources on matters related to identity management and authentication.

## 6.7. Users

Users are:

- Accountable for use of their IT identification and authentication information to access Agency electronic services, resources and information;
- Responsible for protecting and never sharing their CBSA IT identification or authentication information (e.g. user name, password or credentials/tokens); and
- Responsible for reporting any compromise or suspected compromise of their CBSA identity or authentication information to their supervisor and change their password immediately.

## 6.8. Managers

Managers are responsible for:

- Approving the creation of a user account;
- Ensuring that users have the required security clearance; and
- Ensuring that users who require privileges to access Critical systems have at minimum a Secret security clearance.

[1] Based on Treasury Board Secretariat's Cyber Authentication Technology Solutions -Interface Architecture and Specification







# 7. COMPLIANCE AND REPORTING

CBSA is responsible for ensuring that its programs and services are well managed. The Security and Professional Standards Directorate and the IT Security and Continuity Division must actively monitor management practices and controls related to this directive. Where significant deficiencies are encountered or improvements are needed, Agency senior officials will be informed.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Manual - Standard for Security Incident Reporting.

# 8. CONSEQUENCES

The DSO is responsible for investigating and responding to reports of non-compliance with this directive and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies; directives or standards may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment.

## 8.1. Directive Review

The IT Security Coordinator (Director ITSD) should initiate a review of this directive at least every three years, or earlier as required.

# 9. REFERENCES

**Treasury Board Secretariat (TBS)**

- Policy on Government Security - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578
- Directive on Identity Management - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577&section=text
- Standard on Identity and Credential Assurance - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776&section=text
- Guidelines on Defining Authentication Requirements - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=text
- Operational Security Standard: Management of Information Technology Security (MITS) http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text

**Communications Security Establishment Canada (CSEC)**

- IT Security Guidance: User Authentication Guidance for IT Systems - http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html










# 10. ENQUIRIES

Enquiries regarding this standard should be directed to:

| Office Responsible | Contact Information |
|---|---|
| **Information, Science & Technology Branch**<br>IT Security & Continuity Division | **E-mail**: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca<br>**Intranet**: IT Security |
| **Comptrollership Branch**<br>Security and Professional Standards Directorate | **E-mail**: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca |

# 11. ENQUIRIES

Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive relative à la gestion de l'identité et à l'authentification dans les systèmes d'information

**20 janvier 2015**

PROTECTION • SERVICE • INTÉGRITÉ

Canada



# Table des matières









# 1. DATE D'ENTRÉE EN VIGUEUR

La présente directive entre en vigueur le 20 janvier 2015.

# 2. ÉNONCÉ DE LA DIRECTIVE

## 2.1. Objectif

Assurer la diffusion de pratiques efficaces en matière de gestion de l'identité liée aux technologies de l'information (TI) au sein de l'Agence des services frontaliers du Canada afin de protéger les services électroniques, les *systèmes essentiels*, les ressources et les renseignements de l'Agence.

La présente directive est étroitement liée à la Directive sur le contrôle de l'accès aux systèmes d'information.

## 2.2. Résultats attendus

Les résultats attendus de la présente directive sont les suivants :

a) la gestion de l'identité et l'authentification liées aux TI constituent un élément identifiable et font partie intégrale des services électroniques, des systèmes essentiels, des ressources et des renseignements de l'Agence;
b) l'Agence transige avec des *entités* connues lors de la prestation de services électroniques; et
c) l'intégrité de l'identité et l'authentification de l'entité ainsi que les contrôles internes associés atténuent efficacement les risques que des pouvoirs non autorisés soient octroyés et que les activités non autorisées suivantes, liées aux renseignements, aient lieu : l'accès, la divulgation, la destruction, le retrait, la modification et l'usage inapproprié.

# 3. APPLICATION

La présente directive s'applique :

a) à toutes les entités ayant accès aux services électroniques, systèmes essentiels, ressources et renseignements de l'Agence;
b) aux gestionnaires autorisés de l'ASFC chargés de la gestion de l'identité telle qu'énoncée dans la présente Directive.

# 4. CONTEXTE

La Politique sur la sécurité du gouvernement exige que chaque organisation valide de façon adéquate la légitimité de l'identité et des justificatifs de toute personne ou institution avec laquelle elle transige.

L'ASFC doit mettre en œuvre un cadre commun relatif à l'identité et à l'authentification. Les pratiques relatives à la gestion de l'identité doivent être en accord avec l'approche pangouvernementale permettant l'interopérabilité et l'échange de renseignements liés à l'identité des personnes, le cas







échéant, afin d'atteindre les objectifs globaux du gouvernement du Canada et les mandats des ministères.

La présente Directive doit être lue en parallèle avec la Directive sur le contrôle de l'accès aux systèmes d'information de l'ASFC.

# 5. EXIGENCES

a) Tous les systèmes de TI, les applications et les services connexes de l'ASFC doivent être conformes à la présente Directive relative à la gestion de l'identité et à l'authentification dans les systèmes d'information;

b) les utilisateurs doivent se voir attribuer un code d'identification unique (ID utilisateur) créé en conformité avec les normes/politiques en matière de TI qui leur permettra d'accéder à tous les réseaux/systèmes de TI de l'Agence, c.-à-d. l'environnement d'informatique répartie, l'ordinateur central, etc.;

c) en cas de situation hors de l'ordinaire et uniquement avec l'autorisation d'un gestionnaire de niveau 3 ou supérieur et l'accord de la Division de la sécurité et de la continuité de la TI, on pourra octroyer plusieurs ID utilisateurs ou les utilisateurs pourront continuer à utiliser un ID utilisateur non standard lorsque cela est absolument nécessaire pour accomplir les tâches;

d) on attribuera un compte spécial et un code d'identification d'utilisateur unique créé en conformité avec les normes/politiques en matière de TI aux utilisateurs qui ont besoin de privilèges pour accéder aux systèmes de l'ASFC;

e) les utilisateurs doivent détenir une cote de sécurité d'un niveau approprié à leurs fonctions;

f) exception faite de l'accès aux sites Web publics, toutes les entités doivent faire l'objet d'une identification et d'une authentification uniques avant d'obtenir l'accès aux services électroniques, aux ressources et aux renseignements de l'ASFC;

g) les renseignements d'identification et d'authentification sont protégés contre toute divulgation non autorisée; et

h) au besoin, des mécanismes sont mis en œuvre afin de fournir une assurance quant à l'identité et aux justificatifs des entités, y compris des personnes, des organisations et des appareils.

# 6. RÔLES ET RESPONSABILITÉS

## 6.1. Dirigeant principal de l'information (DPI)

Le DPI est chargé de :

- s'assurer que les processus liés à la gestion de l'identité et l'authentification exécutés par les systèmes d'information sont cernés, examinés et validés; et
- désigner un bureau responsable de la coordination des activités liées à l'authentification de l'identité à l'échelle de l'Agence.

## 6.2. Agent de sécurité du ministère (ASM)

L'ASM est chargé :







- d'organiser l'examen de la présente Directive et de coordonner les mises à jour, au besoin;
- d'appuyer les gestionnaires responsables de la prestation des programmes et des services (GPPS) en fournissant, au besoin, des conseils et une orientation à l'égard de l'identité et de l'authentification des utilisateurs;
- de fournir aux gestionnaires, à leur demande, des renseignements concernant la cote de sécurité des utilisateurs;
- de communiquer à tous les utilisateurs des séance d'information sur la sécurité;
- de s'assurer que les certificats de sécurité sont dûment signés par le gestionnaire et l'utilisateur privilégié; et
- de s'assurer que les exigences relatives à la gestion de l'identité dans les systèmes de TI figurant dans la présente Directive, ainsi que les normes et les lignes directrices connexes, sont mises en œuvre à l'échelle de l'Agence.

## 6.3. Coordonnateur de la sécurité de la TI (CSTI)

Le coordonnateur de la sécurité de la TI est chargé :

- de s'assurer que les systèmes des fournisseurs de services possèdent la capacité nécessaire pour satisfaire aux exigences en matière d'identification et d'authentification énoncées dans la présente Directive et dans les normes connexes; et
- d'élaborer de nouveaux instruments de politique liés à l'identité dans les systèmes d'information et de mettre à jour ceux déjà existants.

## 6.4. Gestionnaires responsables de la prestation des programmes et des services (GPPS)

Les GPPS sont chargés de :

- s'assurer que tous les utilisateurs, organisations et appareils devant accéder aux services électroniques, aux ressources et aux renseignements de l'ASFC font l'objet d'une identification et d'une authentification, conformément aux exigences de la présente Directive et des directives, normes et lignes directrices connexes.

## 6.5. Fournisseurs de services externes (y compris le SPC)

Les fournisseurs de services externes doivent :

- respecter la présente Directive de l'ASFC, et les normes connexes dans l'exécution de leurs tâches liées à l'administration des systèmes et des applications de TI de l'ASFC et ne pas les contourner.

## 6.6. Architectes d'entreprise

Les architectes d'entreprise sont chargés de :



- tenir une liste faisant autorité de toutes les solutions liées aux justificatifs d'identité approuvées par l'ASFC[1]; et
- agir à titre d'expert en la matière et fournir des conseils techniques aux GPPS et à leur personnel sur des questions concernant la gestion de l'identité et l'authentification.

### 6.7. Utilisateurs

Les utilisateurs doivent :

- rendre compte de l'utilisation de leur code d'identification et de leurs renseignements d'authentification permettant l'accès aux services électroniques, ressources et renseignements de l'Agence;
- protéger et ne jamais divulguer leur code d'identification et leurs renseignements d'authentification donnant accès aux systèmes de l'ASFC (p. ex. nom d'utilisateur, mot de passe ou justificatifs/jetons d'identité); et
- signaler à leur superviseur toute atteinte, réelle ou soupçonnée, à leur identité ou leurs renseignements d'authentification donnant accès aux systèmes de l'ASFC et changer leur mot de passe immédiatement.

### 6.8. Gestionnaires

Les gestionnaires sont chargés :

- d'approuver la création d'un compte d'utilisateur;
- de s'assurer que les utilisateurs détiennent la cote de sécurité requise; et
- de s'assurer que les utilisateurs qui ont besoin de privilèges pour accéder aux systèmes essentiels détiennent au moins la cote de sécurité « secret ».

## 7. CONFORMITÉ ET RAPPORTS

L'ASFC doit assurer la saine gestion de ses programmes et de ses services. La Direction de la sécurité et des normes professionnelles et la Division de la sécurité et de la continuité de la TI doivent surveiller activement les pratiques et les contrôles liés à la présente Directive. Les hauts fonctionnaires de l'Agence doivent être informés de lacunes importantes ou d'améliorations requises.

Les employés doivent signaler les incidents relatifs à la sécurité conformément aux exigences énoncées dans le Volume de sécurité de l'ASFC – Norme de sécurité matérielle pour le signalement des incidents de sécurité.

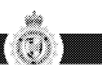
## 8. CONSÉQUENCES

Il incombe à l'ASM d'effectuer des enquêtes sur les cas de non-conformité avec la présente Directive, de répondre à ces signalements et de s'assurer que les mesures appropriées sont prises au besoin. Tout

[1] Fondée sur l'Architecture et spécification de l'interface des Solutions technologiques d'authentification électronique du Secrétariat du Conseil du Trésor.







employé ayant enfreint les politiques, directives ou normes peut faire l'objet d'un examen de sa cote de sécurité et de mesures disciplinaires, lesquelles peuvent aller jusqu'au licenciement.

### 8.1. Examen de la Directive

Le coordonnateur de la sécurité de la TI (directeur de la DSI) devrait examiner la présente Directive au moins aux trois ans, ou plus fréquemment si nécessaire.

## 9. RÉFÉRENCES

**Secrétariat du Conseil du Trésor (SCT)**

- Politique sur la sécurité du gouvernement - http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=16578
- Directive sur la gestion de l'identité :- http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16577&section=text
- Norme sur l'assurance de l'identité et des justificatifs- http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776&section=text
- Ligne directrice sur la définition des exigences en matière d'authentification- http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26262&section=text
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328&section=text

**Centre de la sécurité des télécommunications Canada (CSTC)**

- Guide sur l'authentification des utilisateurs pour les systèmes TI - http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-fra.html

## 10. DEMANDES DE RENSEIGNEMENTS

Veuillez adresser vos demandes de renseignements au sujet de la présente Directive à :

| Bureau responsable | Coordonnées |
|---|---|
| **Direction générale de l'information, des sciences et de la technologie**<br>Division de la sécurité et de la continuité de la TI | **Courriel** : CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca<br>**Intranet** : Sécurité des TI |
| **Direction générale du contrôle**<br>Direction de la sécurité et des normes professionnelles | **Courriel** : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca |



# 11. DÉFINITIONS

Des définitions précises provenant de sources qui font autorité se trouvent dans le Lexique de la terminologie en sécurité.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Directive for the Security of the Computing Environment

**January 20, 2015**









# Contents









# 1. EFFECTIVE DATE

This directive is effective January 20, 2015.

# 2. CONTEXT

The Operational Security Standard on Management of Information Security (MITS) states that IT security is an integral part of continuous program and service delivery. To avoid the loss of service and trust that IT security breaches can cause, departments need to view IT security as a business imperative; a "service enabler."

Therefore, the CBSA's programs and services require that their users and information systems rely on a secure computing environment in order to maintain the confidentiality, integrity and availability of information.

This directive supports the IT Security Policy.

This directive must be read in conjunction with the IT Security Policy and supporting IT Security directives and standards.

# 3. APPLICATION

This directive is applicable to:

- All CBSA management and employees (permanent, term, casual, part-time), contract and private agency personnel, and individuals seconded or assigned to CBSA (including students) and any other individuals required to comply with CBSA policy by virtue of a contract or a memorandum of understanding (MOU).
- External service providers when they store or process CBSA IT information assets (e.g. Shared Service Canada).







# 4. DIRECTIVE STATEMENT

## 4.1. OBJECTIVE

The objective of this directive is to secure all information technology (IT) networks/systems (i.e. the Computing Environment) against threats that have the potential to impact the confidentiality, integrity, availability, intended use and value of the information systems they support. Although overall responsibility remains with the CBSA, a large part of the computing environment is supplied by the CBSA's service provider(s) and thus it is expected that those services providers respect the content of this directive.

## 4.2. EXPECTED RESULTS

The expected results of this directive are:

- Implemented security measures are in place to protect the CBSA's information and assets throughout their life cycle; and
- IT system developers, managers, administrators, analysts, and IT system users are informed of their obligations and responsibilities with respect to the IT systems used and provided by the Agency.

# 5. REQUIREMENTS

The CBSA and the CBSA's service providers of computing environments must ensure that:

- Security safeguards are implemented to secure the Computing Environment, including:
    - All computer systems (e.g. desktops, laptops, notebooks, touchpads, wireless devices), stand-alone or connected to local area networks;
    - Mainframes, distributed and e-commerce environments;
    - Intranet/Internet access;
    - Social Media;
    - Removable media; and
    - Other computing devices utilized by the CBSA.
- Authorized users of the computing environment follow all Agency policy instruments (i.e. policies, directives and standards) that address such areas as, but not limited to:
    - Acceptable use;










- Access control;
- Identity management and Authentication;
- Virus scanning;
- Use of Internet facilities (including Social Media); and
- External email resources.

- Risks related to the Computing Environment are mitigated according to the security assessment and authorization of information systems.

Some security concerns are specific to particular elements of the computing environment, as detailed hereafter.

## 5.1. Infrastructure Components (Mainframe/Distributed/e-Commerce/Network)

Due to the large amount of protected information stored and processed on the Agency systems, the large number of users granted access to this data at various levels, and the integrated dependency between computing platforms, it is important to ensure that all components function harmoniously and do not cause problems with other areas of the computing environments. All components connected to or part of the computing environments must undergo security assessment and authorization (as required) prior to installation and use. This requirement applies to hardware, software (including commercial off-the-shelf «COTS»), applications, etc.

### 5.1.1. Mobile Devices

Only Agency approved and certified mobile devices such as laptops, notebooks, touchpads, etc. are permitted to connect to the Agency's network. They can exchange information with a computer or server through a cellular telephone network, internet or through an infrared link.

The Agency-approved full disk encryption and access control product must be installed on all Agency mobile devices.

As mobile devices are portable and require physical security protection, they must be stored in locked cabinets approved by the Departmental Security Officer (DSO), when not in use. The loss or theft of this equipment is to be considered as a security incident and must be reported accordingly. See Standard for Security Incident Reporting.










### 5.1.2. Personal Digital Assistants (PDAs)

Personal Digital Assistants (PDAs) are comparable to low-performance laptops that can input, process and transmit data.

### 5.1.3. Hardware

Documentation of the current hardware and network configuration must be maintained and reviewed on a regular basis. The documentation shall identify all components and interconnections.

All hardware components shall be documented to capture, at a minimum:

- Manufacturer/supplier;
- Model/version number; and
- Serial number and location of asset.

### 5.1.4. Software

Documentation of the current software components shall be maintained and reviewed on a regular basis. The documentation must identify, at a minimum:

- Manufacturer/supplier;
- Version number;
- Required operating system; and
- Identification and location of the system where installed.

All software used on the CBSA's infrastructure must undergo security assessment and authorization, as required, prior to installation and use. Software must have current valid Agency licenses and must respect all requirements within the license agreements, which include areas such as usage, distribution, copying.

## 5.2. System Development Life Cycle (SDLC)

A System Development Life Cycle (SDLC) methodology must be used for the development or major revision of information systems. A review of the security requirements and compliance to the IT Security policies and standards must be conducted. See IT Security Risk Management Directive.

Procedures that control changes to information systems in production must be documented and implemented. The procedures must include the mechanism for requesting changes, recording and










tracking outstanding requests, approval of requests, testing and documentation of changes and incorporation of the changes.

Procedures must be developed, documented and implemented for the reporting, recording, tracking and resolving of production problems.

Maintenance and repairs to IT systems must be coordinated by Agency IT personnel, who are authorized to perform or arrange for repair and maintenance. Maintenance logs are to be maintained for the life of the asset.

Non-Agency maintenance/repair personnel requiring “short term” access to equipment, software or to areas storing Agency information are to be escorted at all times by authorized Agency personnel.

No client identifiable data is to be used for testing or training purposes without first performing a security assessment or obtaining a waiver approved by the DSO. Test criteria including the use of non-client identifiable test data must be established to ensure adequate quality assurance and end user acceptance testing.

A formal contingency plan must be developed and tested at regular intervals for all critical IT and communications systems.

An IT access control system that verifies the identity, authentication and authorization of system users must be implemented. When system access has been denied, no indication of the reason shall be provided. A log of all invalid access attempts must be maintained and regularly reviewed. See Directive for Access Control in Information Systems.

## 5.3. Remote Work

### 5.3.1. *User of Computers outside CBSA Premises (mobile computing devices)*

This directive applies to all individuals who perform work-related activities from home or from some other off-site location.

Operating systems, such as Microsoft Windows and applications, including Word/Excel/PowerPoint, use the computer’s hard drive as an extension of memory through swap files, temp files, etc. Although usually deleted, it is difficult to ensure that no classified and/or protected information remains on the unprotected hard drive. In addition, as an individual’s private computing device has vulnerabilities, only Agency owned computing devices are to be used for work-related activities such as creating, processing, storing or transmitting information or for accessing Agency networks. This applies to both desktop and mobile computing devices.







Any Agency computing device (desktop or mobile) used off-site must have the appropriate safeguards, such as Agency-approved full disk encryption and access controls in order to protect the confidentiality of the data from deliberate or unauthorized disclosure.

Classified information must not to be removed from, stored (either electronically or physically), processed or used outside Agency premises unless approved by senior management in consultation with the DSO.

Individuals must complete a formal telework arrangement for off-site use of an Agency computing device that will have the appropriate safeguards installed.

Mobile computing devices including but not limited to laptops, notebooks, touchpads, etc. are attractive items that require physical security protection, especially when off Agency premises. Care must be taken to secure these items when not in use. These devices should not be kept in plain view or easily accessible when left unattended. Physical protection of the devices must be ensured as outlined in CBSA Security Manual - Standard for Storage and Transport of Information Assets. The loss or theft of Agency equipment is to be considered as a security incident and must be reported accordingly as outlined in the CBSA Security Manual - Standard for Security Incident Reporting.

### 5.3.2. Secure Remote Access (SRA)

Telecommuting (or telework) is a method of connecting to the office environment for users who frequently perform their duties away from the physical office.

Access to the Agency network from remote locations must be done through approved Agency solution(s) (secure method(s) supported by a security risk assessment and approved by the Office of the DSO, and the Office of the ITSC.

All secure remote access must support:

- Strong and continuous authentication to the network and computing resources;
- Confidentiality of the user's media, local files, and communication to the Agency; and
- Integrity of the remote computer hardware, software, and the data flowing between the remote computer and their enterprise-networking environment.








## 5.4. Internet / Intranet Access

Access to the "internet and the Agency's "intranet" is part of the distributed environment. All users who are part of the distributed network via desktop or Mobile devices have access to the "internet" and to the "intranet".

### 5.4.1. Internet Kiosk / Standalone Access

Access to the "internet" may also be accessible the "Internet Kiosk" where one workstation is shared by multiple users.

There are some exceptions where stand-alone Internet access is required that is not part of the Agency's network, such as Public Access Forms PCs , Labs, etc. Such access requires specific authorization and appropriate safeguards.

### 5.4.2. Unrestricted Internet Access

The Agency's internet solution is restricted in the sense that questionable or suspect sites/categories will be blocked from access.

Unrestricted internet access may be granted for performance of work-related duties by obtaining approval from the DSO and may require the use of a standalone internet connection (separate from the CBSA network).

### 5.4.3. Anonymous Internet Access

When a user has a work-related requirement to have internet access and protection of the user's identity is required, a request can be made for the setup and use of an anonymous Internet account. This solution is not for general internet access but only for those instances where anonymous surfing is a necessary part of the work being performed.

## 5.5. Infrastructure Security

The Protected-B infrastructure of the CBSA is maintained by a service provider(s), while the Classified infrastructure is maintained by CBSA resources. This is subject to change, under the direction of the Treasury Board Secretariat.

### 5.5.1. Malicious Code / Virus Protection



Agency networks and workstations must be protected from the increasing threat of malicious codes and viruses. Virus detection/removal capabilities must be installed at the network/server level and on all workstations (desktop and portable) whether connected to a network or stand-alone system.

Maintenance (updates) of virus detection/removal software must be based upon the service provider's established standards.

All media regardless of internal or external source (including new software) must be scanned prior to installation and use.

### 5.5.2. *Electronic Perimeter Safeguards*

External connectivity for CBSA users must be provided so that the Agency can take advantage of the Internet. However, this provides opportunity for network intrusions and will require that the necessary boundary safeguards (i.e. firewalls) are in place, so that such capability can be used and not put individuals, classified and/or protected information and/or technical resources at risk.

Boundary protection mechanisms (a combination of routers, firewalls, and guards) must be implemented to limit access to the internal network and that only the necessary capabilities are activated. The Agency network defences must be organized in security zones to provide layers of defence.

Stand-alone systems with external connectivity, i.e. to the Internet, etc. must have personal firewall software installed and configured based on SSC's recommendations.

### 5.5.3. *Vulnerability Assessments*

Network assessments are required to determine where and when improvements are needed to the overall network security posture. These preventive measures operate periodically/on demand to examine the system for vulnerabilities that an adversary could exploit. Network penetration testing must be conducted by the network service provider on a regular or routine basis. Where major changes to the Agency's networks, including perimeter defences have been undertaken, it is prudent to test the security merits of such upgrades to determine effectiveness of the infrastructure system's protection.

Network assessment is a requirement at boundary point devices and network hosts to discover known vulnerabilities in host or network system components, and improper configurations visible from the network that create the potential for unauthorized access or exploitation of system resources.

### 5.5.4. *Infrastructure Risk Assessments*







The service provider(s) are responsible for carrying out, and providing to CBSA, Risk Assessments of the computing infrastructure used by CBSA.

### 5.6. Application Vulnerability Management

The CBSA will perform application vulnerability assessments on critical applications as recommended within IT Risk Assessments of those applications.

### 5.7. Monitoring

The Agency networks and systems must be monitored by authorized personnel for operational reasons to determine whether they are operating efficiently, to isolate and resolve problems, and to determine if utilization complies with Agency policies and standards.

The Agency may conduct checks periodically, randomly, and upon request. In any of these instances, information may be analyzed. All information utilizing IT networks/systems that is obtained, stored and/or disseminated is subject to monitoring. The Agency's IT networks include computer systems, personal drives, primary systems such as distributed or mainframe applications and secondary systems such as email or Internet.

The monitoring function may include, but is not limited to, viewing the content and analyzing the volume of files, emails or logs where there is a suspicion of misuse.

The DSO is the functional authority for content monitoring. The policy and requirements concerning content monitoring can be found in the CBSA Security Volume, Policy on the Use of Electronic Resources and Directive on the Appropriate Use of E-mail.

## 6. ROLES & RESPONSIBILITIES

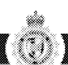
### 6.1. Chief Information Officer (CIO)

The CIO is responsible for:

- Ensuring that the computing environment safeguards are deployed and maintained as required; and
- Ensuring that computing environment service providers (including CRA and SSC) deploy and maintain required safeguards for the computing environment.







## 6.2. Departmental Security Officer (DSO)

The DSO is responsible for:

- Providing subject matter expertise and consultation to stakeholders on matters related to information security; and
- Investigating and responding to reports of non-compliance with this directive.

## 6.3. IT Security Coordinator (ITSC)

The IT Security Coordinator is responsible for (including ensuring that computing environment service providers):

- Ensuring that security assessments for information systems cover the underlying computing environment components, as required;
- Providing guidance to facilitate the definition, deployment and maintenance of security safeguards to the computing environment;
- Liaising with external providers (e.g. SSC, CSEC, TBS) to ensure a whole-of-government approach to security of the computing environment; and
- Providing subject matter expertise and technical consultation to Program and Service Delivery Managers (PSDMs) and their resources on matters related to security of the computing environment.

## 6.4. Program and Service Delivery Managers (PSDMs)

PSDMs are responsible for:

- Ensuring that requirements for the security of the computing environment are met when deploying their information systems; and
- Planning, programming, and budgeting for security in their information systems.

## 6.5. Computing Environment Service Providers (including CRA and SSC)

Computing environment Service Providers are responsible for:

- Adhering to this directive and ensuring that its requirements are met when providing products and services to CBSA.

## 6.6. Users

Users are responsible for:

- Adhering to this directive and ensuring its requirements are met;
- Using their CBSA provided resources according to CBSA policy requirements; and










- Reporting any compromise or suspected compromise of their CBSA identity or authentication information to their supervisor and change their password immediately.

# 7. COMPLIANCE AND REPORTING

The Departmental Security Officer, the IT Security Coordinator, security practitioners and managers are responsible for monitoring compliance with this directive within CBSA, measuring the effectiveness of securing the CBSA's computing environments and ensuring appropriate remedial actions are taken when deficiencies arise.

Employees must report security incidents in accordance with the requirements outlined in the CBSA Security Manual - Reporting of Security Incidents.

# 8. CONSEQUENCES

The DSO is responsible for investigating and responding to reports of non-compliance with this directive and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies; directives or standards may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment.

# 9. DIRECTIVE REVIEW

The IT Security Coordinator (Director ITSD) should initiate a review of this directive at least every three years, or earlier as required.

# 10. REFERENCES

**Treasury Board Secretariat (TBS)**

- Policy on Government Security (PGS) – http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578
- Directive on Departmental Security Management (DDSM) – http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579&section=text





- Operational Security Standard: Management of Information Technology Security (MITS) - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text

**Communications Security Establishment Canada (CSEC)**

- ITSG - IT Security Risk Management: A Lifecycle Approach (ITSG-33) - https://www.cse-cst.gc.ca/en/node/265/html/22814

**Other CBSA Policies/Directives.**

## 11. ENQUIRIES

Enquiries regarding this directive should be directed to:

Information, Science and Technology Branch
**IT Security Coordinator, IT Security and Continuity Division**

E-mail: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca

Intranet: http://atlas/istb-dgist/services/it-ti-sec/it_ti_sec_eng.asp

## 12. DEFINITIONS

Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive relative à la sécurité de l'environnement Informatique

**20 JANVIER 2015**

PROTECTION • SERVICE • INTÉGRITÉ

Canada



## Table des matières



# 1. DATE D'ENTRÉE EN VIGUEUR

La présente directive entre en vigueur le 20 janvier 2015.

# 2. CONTEXTE

Selon la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information, la sécurité des TI fait partie intégrante de la prestation continue de programmes et de services. Pour éviter toute interruption de service ou perte de confiance que pourrait causer une atteinte à la sécurité des TI, les ministères sont tenus de concevoir la sécurité des TI comme étant un impératif opérationnel et un outil de prestation de services.

En conséquence, les utilisateurs et systèmes d'information soutenant les programmes et les services de l'ASFC doivent s'appuyer sur un environnement informatique sûr afin d'assurer la confidentialité, l'intégrité et la disponibilité des renseignements.

La présente directive appuie la Politique sur la sécurité des TI.

La présente directive doit être lue en parallèle avec la Politique sur la sécurité des TI et les directives et normes connexes en matière de sécurité des TI.

# 3. APPLICATION

La présente directive s'applique :

- à tous les gestionnaires et employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), aux sous-traitants et au personnel d'agences privées ainsi qu'au personnel en détachement ou en affectation à l'ASFC (y compris les étudiants) et à toute autre personne devant se conformer aux politiques de l'ASFC en vertu d'un contrat ou d'un protocole d'entente (PE);
- aux fournisseurs de services externes lorsqu'ils traitent ou conservent des biens de TI de l'ASFC (p. ex., Services partagés Canada).

# 4. ÉNONCÉ DE LA DIRECTIVE

## 4.1. OBJECTIF

L'objectif de la présente directive est de protéger tous les réseaux/systèmes de technologie de l'information (TI) (c.-à-d. l'environnement informatique) contre toute menace susceptible de porter atteinte à la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des systèmes d'information qu'ils soutiennent. Bien que l'ASFC en ait la responsabilité générale, l'environnement informatique est en grande partie fourni par ses fournisseurs de services, et il est attendu que ces derniers respectent la présente directive.







## 4.2. RÉSULTATS ATTENDUS

Les résultats attendus de la présente directive sont les suivants :

- la mise en place de mesures de sécurité pour protéger les informations et les biens de l'ASFC tout au long de leur cycle de vie; et
- les développeurs, gestionnaires, administrateurs, analystes et utilisateurs de systèmes de TI connaissent leurs obligations et leurs responsabilités concernant les systèmes de TI utilisés et fournis par l'Agence.

# 5. EXIGENCES

L'ASFC et ses fournisseurs de services d'environnement informatique doivent s'assurer que :

- des mesures de sécurité sont mises en œuvre afin de protéger l'environnement informatique, y compris :
    - tous les systèmes informatiques (p. ex. les ordinateurs de bureau, portatifs, bloc-notes, tablettes électroniques et appareils sans fil), autonomes ou reliés à des réseaux locaux;
    - les ordinateurs centraux, les environnements d'informatique répartie et de commerce électronique;
    - les accès à l'intranet/Internet;
    - les médias sociaux;
    - les supports amovibles; et
    - les autres appareils électroniques utilisés par l'ASFC.
- les utilisateurs autorisés de l'environnement informatique respectent les instruments de politique de l'ASFC (c.-à-d. les politiques, les directives et les normes) concernant, notamment, les points suivants :
    - l'utilisation acceptable;
    - le contrôle de l'accès;
    - la gestion de l'identité et l'authentification;
    - la détection de virus;
    - l'utilisation d'Internet (y compris des médias sociaux); et
    - les services de courriel externes.
- les risques liés à l'environnement informatique sont atténués selon l'évaluation et l'autorisation des systèmes d'information.

Certaines préoccupations sont liées à des composantes particulières de l'environnement informatique décrites ci-dessous.





## 5.1. Composantes de l'infrastructure (ordinateur central, informatique répartie, commerce électronique et réseau)

En raison des grandes quantités de renseignements protégés conservés et traités par les systèmes de l'ASFC, du grand nombre d'utilisateurs à différents niveaux de l'organisation ayant accès à ces données et de la dépendance inhérente entre les plateformes électroniques, il est important de s'assurer que toutes les composantes fonctionnent de façon harmonieuse et ne causent pas de problèmes dans d'autres dimensions de l'environnement informatique. Toutes les composantes reliées à l'environnement informatique ou à une de ses parties doivent être soumises à une évaluation de la sécurité et une autorisation (au besoin) avant leur installation et leur utilisation. Cette exigence vise le matériel, les logiciels (y compris ceux vendus dans le commerce), les applications, etc.

### 5.1.1. Appareils mobiles

Il n'est possible d'accéder au réseau de l'Agence qu'à l'aide d'appareils mobiles (ordinateurs portatifs, bloc-notes, tablettes électroniques, etc.) approuvés et certifiés par l'Agence. Ils permettent d'échanger de l'information avec un ordinateur ou un serveur par réseau téléphonique cellulaire, Internet ou liaison infrarouge.

Un produit de chiffrement et de contrôle d'accès s'appliquant au contenu entier du disque dur et approuvé par l'Agence doit être installé dans tous les appareils mobiles.

Vu que les appareils mobiles sont portatifs et nécessitent un dispositif de sécurité matériel, on doit les ranger dans une armoire verrouillée, approuvée par l'agent de sécurité du ministère (ASM), lorsqu'ils ne sont pas utilisés. Leur vol ou leur perte doit être considéré comme un incident de sécurité et, en conséquence, doit être signalé. Veuillez consulter le document intitulé Norme de sécurité matérielle pour le signalement des incidents de sécurité.

### 5.1.2. Assistants numériques personnels

On peut comparer les assistants numériques personnels à des ordinateurs portatifs à faible rendement pouvant recevoir, traiter et transmettre des données.

### 5.1.3. Matériel

On doit tenir à jour et vérifier régulièrement la documentation concernant le matériel et la configuration du réseau actuels. La documentation doit permettre d'identifier toutes les composantes et les interconnexions.

On doit documenter toutes les composantes matérielles et indiquer, au moins :

- le fabricant/fournisseur;
- le modèle/la version; et
- l'emplacement et le numéro de série du bien.

### 5.1.4. Logiciels



On doit tenir à jour et vérifier régulièrement la documentation concernant les logiciels. La documentation doit contenir au moins :

- le fabricant/fournisseur;
- la version;
- le système d'exploitation requis; et
- le nom du système et l'endroit où il est installé.

Tous les logiciels utilisés dans l'infrastructure de l'ASFC doivent être soumis à une évaluation de la sécurité et une autorisation avant leur installation et leur utilisation. Chaque logiciel doit être assorti d'une licence valide et à jour appartenant à l'ASFC, et toutes les exigences à l'égard, entre autres, de son utilisation, sa distribution et sa copie, énoncées dans la licence doivent être respectées.

## 5.2. Cycle de développement des systèmes (CDS)

Pour élaborer ou réaménager de façon importante un système de TI, on doit adopter la technique du Cycle de développement des systèmes (CDS). On doit examiner la conformité aux exigences en matière de sécurité et aux politiques et normes de sécurité des TI. Veuillez consulter Directive sur la gestion des risques liés à la sécurité des TI.

On doit documenter et mettre en œuvre les procédures régissant les modifications apportées aux systèmes d'information en production. Ces procédures doivent comporter le mécanisme pour demander des modifications, enregistrer et suivre les demandes en suspens, approuver les demandes, tester et documenter les modifications et incorporer celles-ci.

On doit élaborer, documenter et mettre en œuvre des procédures pour signaler, consigner, suivre et résoudre les problèmes de production.

La maintenance et les réparations des systèmes de TI doivent être coordonnées par un membre du personnel des TI autorisé. On doit tenir un registre de maintenance durant tout le cycle de vie d'un actif.

Le personnel de maintenance ou de réparation ne travaillant pas à l'Agence et qui a besoin d'avoir accès pendant une courte période à du matériel, du logiciel ou des lieux de stockage de l'information à l'Agence doit être accompagné en tout temps par un membre du personnel de l'Agence autorisé.

Aucune donnée se rapportant à un client identifiable ne doit servir à des essais ou à de la formation avant qu'on ait effectué une évaluation de la sécurité ou obtenu une dérogation de la part de l'ASM. Des critères d'essai comprenant l'utilisation de données d'essai ne se rapportant pas à un client identifiable devraient être adoptés pour instaurer une assurance adéquate de la qualité et permettre à l'utilisateur final d'effectuer des essais d'acceptation.

On doit établir et tester régulièrement un plan d'urgence officiel couvrant tous les systèmes de TI et de communication essentiels.

On doit mettre en place un système de contrôle d'accès qui vérifie l'identité, l'authentification et l'autorisation des utilisateurs des différents systèmes. Lorsque l'accès à un système est bloqué, aucune raison ne doit en être indiquée. On doit tenir un registre de toutes les tentatives d'accès avortées et







l'examiner régulièrement. Veuillez consulter Directive sur le contrôle de l'accès aux systèmes d'information.

## 5.3. Télétravail

### 5.3.1. *Utilisateurs d'ordinateurs hors des locaux de l'ASFC (appareils informatiques mobiles)*

La présente directive s'applique à toutes les personnes qui mènent des activités liées à leurs fonctions à partir de leur domicile ou d'un autre endroit situé à l'extérieur des locaux de l'ASFC.

Les systèmes d'exploitation, tels que Windows de Microsoft et ses applications, y compris Word/Excel/PowerPoint, utilisent le disque dur de l'ordinateur comme extension de la mémoire vive pour stocker des fichiers d'échange, des fichiers temporaires, etc. Bien que ces fichiers soient habituellement supprimés, il est difficile de s'assurer qu'il ne reste aucune information classifiée et/ou protégée sur le disque dur non protégé. De plus, comme un appareil informatique personnel est vulnérable, seuls les appareils informatiques appartenant à l'Agence peuvent être utilisés pour mener des activités liées au travail, telles que créer, traiter, sauvegarder ou transmettre des informations ou accéder aux réseaux de l'Agence. Cette règle s'applique à la fois aux ordinateurs de bureau et aux appareils informatiques mobiles.

Tout appareil informatique (ordinateur de bureau ou portatif) de l'Agence employé hors de ses locaux doit être doté des protections appropriées, p. ex. le chiffrement et des contrôles d'accès pour le contenu entier du disque approuvés par l'Agence, qui protègent l'intégrité et la confidentialité des données contre toute divulgation délibérée ou non autorisée.

L'information classifiée ne doit pas être éliminée, stockée (électroniquement ni matériellement), traitée ni utilisée hors des locaux de l'Agence, à moins qu'un gestionnaire supérieur ne l'autorise, après consultation de l'ASM.

On doit conclure une entente officielle de télétravail pour utiliser un appareil informatique de l'Agence doté des protections appropriées hors de ses locaux.

Les appareils portatifs tels que les portables, les blocs-notes et les tablettes électroniques sont attrayants mais nécessitent une protection matérielle, particulièrement hors des locaux de l'Agence. Lorsqu'on ne les utilise pas, on doit en assurer la sécurité. On ne doit pas les laisser à la vue, ni facilement accessibles lorsqu'on s'en éloigne. La protection physique des appareils doit être assurée conformément aux exigences énoncées dans le Volume de sécurité de l'ASFC – Norme sur le stockage et le transport de ressources d'information. La perte ou le vol d'équipement appartenant à l'Agence doit être considéré comme un incident de sécurité et, en conséquence, doit être signalé. Veuillez consulter le document intitulé Norme de sécurité matérielle pour le signalement des incidents de sécurité du Volume de sécurité de l'AFSC.

### 5.3.2. *Accès à distance protégé (ADP)*

Le travail à distance (ou télétravail) est un mode de connexion entre le milieu de travail et des utilisateurs qui ont souvent à remplir leurs fonctions ailleurs qu'à leur poste de travail normal.



L'accès au réseau de l'Agence à partir d'endroits distants doit s'effectuer au moyen d'une solution de TI approuvée par l'Agence ou une technique sécuritaire fondée sur une évaluation des risques de sécurité et approuvée par les bureaux de l'ASM et du CSTI.

Tout accès à distance protégé doit assurer en permanence :

- l'authentification parfaite auprès du réseau et des ressources informatiques;
- la confidentialité des médias de l'utilisateur, de ses fichiers locaux et de sa communication auprès de l'Agence; et
- l'intégrité du matériel de télétraitement informatique, des logiciels ainsi que des données échangées entre l'ordinateur à distance et l'environnement de réseautage de son ministère.

## 5.4. Accès à Internet/l'intranet

L'accès à Internet et à l'intranet de l'Agence fait partie de l'environnement d'informatique répartie. Tous les utilisateurs ayant accès au réseau réparti par l'entremise d'un ordinateur de bureau ou d'appareils mobiles ont accès à Internet et à l'intranet.

### *5.4.1. Kiosque de services Internet / accès autonome*

Il est possible d'accéder à Internet par l'entremise d'un kiosque de services Internet, soit un poste de travail partagé par de multiples utilisateurs.

Il existe certaines exceptions où un accès autonome à Internet ne faisant pas partie du réseau de l'Agence est nécessaire, par exemple un accès public à partir d'un ordinateur de bureau ou un laboratoire informatique. De tels accès requièrent une autorisation particulière et des mesures de protection appropriées.

### *5.4.2. Accès Internet sans restrictions*

La solution Internet de l'Agence est restreinte puisque l'accès à des sites suspects ou à des catégories de sites est bloqué.

Il est possible d'obtenir un accès à Internet sans restrictions pour effectuer des tâches liées aux fonctions sur approbation de l'ASM; une connexion autonome à Internet (séparée du réseau de l'ASFC) pourrait être nécessaire.

### *5.4.3. Accès anonyme à Internet*

Dans le cas où les fonctions d'un utilisateur exigent un accès à Internet et qu'il faut protéger son identité, on peut demander un compte Internet anonyme. Cette solution s'applique non pas à l'accès général à Internet, mais uniquement aux cas où l'employé, de par ses fonctions, doit pouvoir naviguer sur Internet de façon anonyme.







## 5.5. Sécurité de l'infrastructure

L'infrastructure Protégé B de l'ASFC est soutenue par un ou plusieurs fournisseurs de services, alors que l'infrastructure Classifié est soutenue par le personnel de l'ASFC. Cet état des choses pourrait changer, selon les directives émises par le Secrétariat du Conseil du Trésor.

### 5.5.1. Code malveillant/protection contre les virus

On doit protéger les réseaux et les postes de travail de l'Agence contre la menace croissante de codes malveillants et de virus. On doit doter de moyens de détection et de suppression de virus les réseaux et les serveurs ainsi que tous les postes de travail (ordinateurs de bureau et portatifs), qu'ils soient reliés à un réseau ou non.

La tenue à jour des logiciels de détection et de suppression de virus doit se fonder sur les normes établies par le fournisseur de services.

On doit analyser tous les supports avant de les installer ou de les utiliser, qu'ils soient d'origine interne ou externe (y compris tout nouveau logiciel).

### 5.5.2. Protections périmétriques électroniques

La connectivité externe offerte aux utilisateurs de l'ASFC doit permettre à l'Agence de tirer avantage d'Internet. Toutefois, cette fonctionnalité augmente le risque d'intrusions dans le réseau et exige que les protections périmétriques nécessaires (p. ex. pare-feu) soient en place afin de permettre de l'utiliser sans pour autant exposer aux risques les personnes, les informations classifiées et/ou protégées et/ou les ressources techniques.

On doit mettre en place des mécanismes de protection périmétriques (une combinaison de routeurs, de pare-feu et de protections) afin de limiter l'accès au réseau interne et d'activer uniquement les fonctionnalités nécessaires. Les défenses du réseau de l'Agence doivent être organisées selon des zones afin de fournir différents niveaux de défense.

Les systèmes autonomes dotés d'une connectivité externe, par exemple à Internet, doivent être munis d'un logiciel pare-feu personnel, et leur configuration doit suivre les recommandations de SPC.

### 5.5.3. Évaluations de la vulnérabilité

On doit évaluer la vulnérabilité des réseaux afin de déterminer à quel endroit et à quel moment il faut les améliorer pour en rehausser la sécurité générale. De telles mesures préventives, qu'elles soient périodiques ou ponctuelles, visent à rechercher dans un système toute faille dont pourrait tirer parti une personne mal intentionnée. Le fournisseur de services de réseau doit vérifier régulièrement si quelqu'un a pénétré dans le réseau. Lorsque des modifications d'envergure ont été apportées aux réseaux de l'Agence, notamment pour en accroître la protection périmétrique, il est prudent d'en vérifier l'avantage sur le plan de la sécurité pour établir l'efficacité de la protection de l'infrastructure.

On doit absolument évaluer la vulnérabilité d'un réseau aux dispositifs de ses points limites et au niveau de ses hôtes pour repérer des faiblesses connues chez son hôte ou des composants système ou détecter







une imperfection de configuration visible depuis le réseau et créant la possibilité d'un accès non autorisé ou d'une exploitation des ressources d'un système.

#### 5.5.4. Évaluation des risques relatifs à l'infrastructure

Il incombe aux fournisseurs de services de mener des évaluations des risques de l'infrastructure informatique utilisée par l'ASFC et de les lui fournir.

### 5.6. Gestion de la vulnérabilité des applications

L'ASFC mènera des évaluations de la vulnérabilité des applications essentielles tel que recommandé dans les évaluations des risques liés aux TI des applications en question.

### 5.7. Surveillance

Les réseaux et les systèmes de l'Agence doivent être surveillés par les membres autorisés du personnel pour des raisons opérationnelles, afin qu'ils établissent si les activités sont efficaces, qu'ils relèvent et règlent les problèmes, et qu'ils déterminent si l'utilisation est conforme aux politiques et aux normes de l'Agence.

L'Agence peut effectuer des vérifications à l'occasion, de façon aléatoire et sur demande. Dans tous les cas, on peut analyser l'information. Toute information utilisant un réseau ou système de TI obtenue, stockée ou diffusée est assujettie à une surveillance. Les réseaux de TI de l'Agence comprennent notamment des systèmes informatiques, des disques durs personnels, des systèmes primaires tels que des applications distribuées ou exécutées sur ordinateur central ainsi que des systèmes auxiliaires tels que le courriel ou Internet.

La fonction de surveillance peut consister, entre autres, à examiner le contenu et le volume de fichiers, de courriels et de registres lorsqu'on soupçonne qu'ils peuvent être utilisés à mauvais escient.

L'ASM est l'autorité responsable de la surveillance du contenu. La politique et les exigences à l'égard de la surveillance du contenu sont énoncées dans le Volume de sécurité de l'ASFC – Politique sur l'utilisation des ressources électroniques et dans la Directive sur l'utilisation appropriée du courrier électronique.

## 6. RÔLES ET RESPONSABILITÉS

### 6.1. Dirigeant principal de l'information (DPI)

Le DPI est chargé de :

- s'assurer que les protections de l'environnement informatique sont en place et sont mises à jour au besoin; et
- s'assurer que les fournisseurs de services d'environnement informatique (y compris l'ARC et SPC) installent et tiennent à jour les protections de l'environnement informatique nécessaires.







## 6.2. Agent de sécurité du Ministère (ASM)

L'ASM est chargé :

- d'agir à titre d'expert en la matière et de fournir des conseils techniques aux intervenants sur des questions concernant la sécurité des renseignements; et
- d'effectuer des enquêtes sur les cas de non-conformité avec la présente directive, et de répondre à ces signalements.

## 6.3. Coordonnateur de la sécurité de la TI (CSTI)

Le coordonnateur de la sécurité de la TI est chargé (y compris de s'assurer que les fournisseurs de services d'environnement informatique se chargent) :

- de s'assurer que les évaluations de la sécurité des systèmes d'information portent sur les composantes sous-jacentes de l'environnement informatique, au besoin;
- de fournir une orientation afin de faciliter l'établissement, la mise en place et la maintenance des protections de l'environnement informatique;
- d'assurer la liaison avec des fournisseurs externes (p. ex. SPC, le CSTC et le SCT) afin de veiller à l'application d'une approche pangouvernementale à la sécurité de l'environnement informatique; et
- d'agir à titre d'expert en la matière et de fournir des conseils techniques aux gestionnaires responsables de la prestation des programmes et des services et à leur personnel sur des questions concernant la sécurité de l'environnement informatique.

## 6.4. Gestionnaires responsables de la prestation des programmes et des services (GPPS)

Les GPPS sont chargés de :

- s'assurer que les exigences en matière de sécurité de l'environnement informatique sont satisfaites au moment de déployer des systèmes d'information; et
- d'assurer la planification, la programmation et les prévisions budgétaires à l'égard de la sécurité des systèmes d'information dont ils sont responsables.

## 6.5. Fournisseurs de services d'environnement informatique (y compris l'ARC et SPC)

Les fournisseurs de services d'environnement informatique doivent :

- respecter la présente directive et s'assurer de satisfaire aux exigences énoncées lors de la prestation de produits et de services à l'ASFC.

## 6.6. Utilisateurs

Les utilisateurs doivent :

- respecter la présente directive et s'assurer de satisfaire aux exigences énoncées;
- faire usage des ressources fournies par l'ASFC conformément aux exigences énoncées dans les politiques; et







- signaler à leur superviseur toute atteinte, réelle ou soupçonnée, à leur identité ou leurs renseignements d'authentification donnant accès aux systèmes de l'ASFC et changer leur mot de passe immédiatement.

# 7. CONFORMITÉ ET RAPPORTS

L'agent de sécurité du Ministère, le coordonnateur de la sécurité de la TI, les gestionnaires et les responsables de la sécurité sont responsables de veiller à la conformité avec la présente directive au sein de l'ASFC, de mesurer l'efficacité de la protection des environnements informatiques de l'ASFC et de s'assurer que les mesures appropriées sont prises lorsque des lacunes sont révélées.

Les employés doivent signaler les incidents relatifs à la sécurité conformément aux exigences énoncées dans le Volume de sécurité de l'ASFC – Norme de sécurité matérielle pour le signalement des incidents de sécurité.

# 8. CONSÉQUENCES

Il incombe à l'ASM d'effectuer des enquêtes sur les cas de non-conformité avec la présente directive, de répondre à ces signalements et de s'assurer que les mesures appropriées sont prises au besoin. Tout employé ayant enfreint les politiques, directives ou normes peut faire l'objet d'un examen de sa cote de sécurité et de mesures disciplinaires, lesquelles peuvent aller jusqu'au licenciement.

# 9. EXAMEN DE LA DIRECTIVE

Le coordonnateur de la sécurité de la TI (directeur de la DSI) devrait examiner la présente directive au moins aux trois ans, ou plus fréquemment si nécessaire.

# 10. RÉFÉRENCES

**Secrétariat du Conseil du Trésor (SCT)**

- Politique sur la sécurité du gouvernement – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=16578
- Directive sur la gestion de la sécurité ministérielle – http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16579&section=text
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328&section=text





**Centre de la sécurité des télécommunications Canada (CSTC)**

- Aperçu de la gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)- https://www.cse-cst.gc.ca/fr/node/265/html/22814

**Autres politiques/directives de l'ASFC.**

## 11. DEMANDES DE RENSEIGNEMENTS

Veuillez adresser vos demandes de renseignements au sujet de la présente directive à :

Direction générale de l'information, des sciences et de la technologie
**Coordonnateur de la sécurité de la TI, Division de la sécurité et de la continuité de la TI**

Courriel : CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca

Intranet : http://atlas/istb-dgist/services/it-ti-sec/it_ti_sec_fra.asp

## 12. DÉFINITIONS

Des définitions précises provenant de sources qui font autorité se trouvent dans le Lexique de la terminologie en sécurité.

Agence des services frontaliers du Canada | Canada Border Services Agency




Direction générale du contrôle

Direction de la sécurité et des normes professionnelles

Division de la coordination des programmes et de la politique en matière de sécurité

Direction générale de l'information, des sciences et de la technologie

Direction des services organisationnels

Division de la sécurité et de la continuité des opérations des TI

# Agence des services frontaliers du Canada (ASFC) Directive sur la gestion des risques liés à la sécurité des technologies de l'information (TI)

Version : 2.0

PROTECTION • SERVICE • INTÉGRITÉ

# Table des matières


Agence des services frontaliers du Canada | Canada Border Services Agency




# DIRECTIVE SUR LA GESTION DES RISQUES LIÉS À LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION (TI)

## 1 DATE D'ENTRÉE EN VIGUEUR

La présente directive entre en vigueur le 20 janvier 2015.

## 2 DIRECTIVE

La présente directive remplace le chapitre 20, Politique sur la Gestion des risques pour la sécurité – Évaluation de la menace et des risques des technologies de l'information et le chapitre 21, Politique des Examens de la sécurité et inspections des systèmes des technologies de l'information, du Volume de sécurité de l'ASFC.

## 3 CONTEXTE

Aux termes de la Politique sur la sécurité du gouvernement (PSG), la gestion de la sécurité exige une évaluation continue des risques ainsi que la mise en place, la surveillance et le maintien de mécanismes appropriés de contrôle de gestion interne en matière de prévention, de détection, d'intervention et de rétablissement. La PSG précise aussi que c'est lorsqu'elle fait partie intégrante des activités, des programmes et de la culture d'un ministère et de la fonction publique dans son ensemble que la gestion de la sécurité est la plus efficace.

La gestion des risques liés à la sécurité des TI est une composante essentielle du Programme de sécurité des TI de l'ASFC, qui vise à assurer la protection des activités opérationnelles et des fonds de renseignements de l'Agence. Grâce à l'application d'un cadre de gestion des risques liés à la sécurité des TI, on peut continuellement contrôler et évaluer les risques qui pèsent sur l'Agence afin que ses programmes et services et les systèmes d'information connexes soient exposés à un niveau de risque acceptable.

Les activités de gestion des risques liés à la sécurité des TI de l'ASFC appuient son cadre de gestion intégrée des risques puisqu'elles constituent un processus continu, proactif et systématique lui permettant de comprendre, de gérer et de communiquer les risques liés à la sécurité des TI d'un point de vue organisationnel.

Pour être vraiment efficace, la gestion des risques liés à la sécurité des TI doit être un processus continu réalisé à tous les niveaux du cycle de vie d'un système ou d'une application.

## 4 APPLICATION

La présente Directive sur la gestion des risques liés à la sécurité des TI s'applique aux intervenants responsables de la sélection, de l'élaboration, de la mise en œuvre et de la maintenance des ressources électroniques de l'ASFC composées de réseaux, de systèmes, d'applications et de données de TI.

Lorsque l'Agence communique des renseignements par voie électronique ou est inter reliée par voie électronique avec d'autres organisations, elle travaille en collaboration avec ses partenaires, clients et intervenants clés pour appliquer la présente Directive dans le cadre de leur relation de travail mutuelle et de l'application continue des activités de gestion des risques liés à la sécurité des TI.

## 5 ÉNONCÉ DE LA DIRECTIVE

Les services, les ressources et les renseignements électroniques de l'Agence sont protégés grâce à un cadre de gestion des risques liés à la sécurité des TI efficace.

### 5.1 OBJECTIFS

Les objectifs de la présente Directive sur la gestion des risques liés à la sécurité des TI sont les suivants :

a) s'assurer que la gestion des risques liés à la sécurité des TI est une composante permanente et intégrante de toutes les activités de l'Agence liées aux systèmes d'information;
b) s'assurer que tous les intervenants pertinents comprennent leurs rôles et responsabilités connexes en lien avec la gestion des risques liés à la sécurité des TI;
c) définir les besoins en matière de sécurité des TI de l'Agence ainsi que ses contrôles de sécurité.

### 5.2 RÉSULTATS ATTENDUS

Les résultats attendus de la présente Directive sont les suivants :

a) les risques liés à l'utilisation inappropriée des services, ressources et renseignements électroniques de l'Agence sont atténués efficacement et gérés continuellement;
b) on adopte une approche organisationnelle pour garantir l'évaluation et le contrôle continus des risques liés à la sécurité des TI associés aux actifs de TI de l'ASFC;
c) la gestion des risques liés à la sécurité des TI est une partie intégrante et visible des responsabilités et de l'imputabilité de la direction de l'Agence.

## 6 EXIGENCES

Une gestion des risques liés à la sécurité des TI efficace exige que :

a) les besoins opérationnels en matière de sécurité sont cernés et documentés;
b) les contrôles de sécurité sont définis et évalués pour les composantes communes (p. ex. gestion des incidents, contrôle du rendement et gestion de l'identité) à l'appui des systèmes d'information;
c) l'Agence utilise les évaluations de la menace pour veiller à mettre en œuvre des systèmes d'information qui satisfont aux exigences de l'ASFC en matière de sécurité des TI;
d) l'ASFC élabore des profils de contrôle de sécurité adaptés à ses besoins opérationnels en matière de sécurité dont on peut tirer profit dans le cadre des projets de TI au moment de mettre en œuvre et de mettre à niveau les systèmes d'information de l'Agence;
e) le rendement des contrôles de sécurité des TI appliqués au sein de l'Agence fait l'objet d'un contrôle et d'une évaluation continus;
f) les vulnérabilités et les faiblesses sont cernées;

g) on élabore et prend des mesures correctives contenues dans les plans d'action de la gestion (PAG) pour s'assurer que les vulnérabilités et les faiblesses sont éliminées et pour améliorer le rendement et la situation générale de l'Agence en matière de sécurité.

## 7 RÔLES ET RESPONSABILITÉS ET IMPUTABILITÉ

La gestion des risques liés à la sécurité est plus efficace lorsqu'on bénéficie de la participation et de la collaboration de tous les intervenants nécessaires pour s'acquitter des tâches décrites ci-dessous.

**Dirigeant principal de l'information (DPI)**

Le vice-président (VP) de la DGIST a été nommé DPI. Parmi les responsabilités du DPI, mentionnons les suivantes :

- créer une relation productive et fonctionnelle entre l'agent de sécurité du ministère (ASM) et le coordonnateur de la sécurité de la TI (CSTI) en vue d'établir une approche coordonnée et intégrée à l'égard de la mise en œuvre des exigences du programme de sécurité;
- veiller à l'application de contrôles de sécurité appropriés à tous les biens et processus et à toutes les activités de la technologie et de la gestion de l'information de l'Agence;
- s'assurer que le coordonnateur de la sécurité de la TI fournit des séances d'information régulières au DPI et à l'ASM concernant les risques liés à la sécurité des TI de l'organisation.

**Agent de sécurité du ministère (ASM)**

Le directeur général (DG) de la Direction de la sécurité et des normes professionnelles (DSNP) a été nommé ASM. L'ASM élabore, met en œuvre, contrôle et tient un plan de sécurité ministériel (PSM) et est responsable de la gestion du programme de sécurité de l'Agence. L'ASM a les responsabilités suivantes :

- accepter les risques liés à la sécurité à l'échelle de l'Agence;
- intégrer les besoins opérationnels en matière de sécurité, les résultats de l'évaluation des menaces de l'Agence, les objectifs de l'Agence en matière de contrôle de sécurité et les contrôles de sécurité dans le PSM aux fins d'approbation par le président de l'ASFC (administrateur général);
- mettre à jour le PSM pour refléter les changements apportés aux besoins opérationnels en matière de sécurité, les objectifs de contrôle de sécurité et les exigences connexes;
- superviser la réalisation des activités de gestion des risques liés à la sécurité des systèmes d'information proposées;
- avec l'aide du CSTI, élaborer et promouvoir l'utilisation de profils de contrôle de sécurité de domaine touchant la mise en œuvre des systèmes d'information de l'Agence dans le cadre de tous les projets de TI de l'ASFC.

**Coordonnateur de la sécurité de la TI (CSTI)**

Le directeur de la Division de la sécurité et de la continuité des opérations des TI (DSCOTI) est nommé coordonnateur de la sécurité de la TI (CSTI). Le CSTI doit établir et gérer une fonction de sécurité des TI au sein du programme de sécurité de l'Agence et il a les responsabilités suivantes :

- établir et gérer le volet sécurité des TI dans le cadre du programme coordonné de sécurité de l'Agence;

- examiner et recommander l'approbation de politiques et de normes de sécurité des TI de l'Agence et toutes les politiques qui ont des répercussions sur la sécurité des TI;
- travailler en étroite collaboration avec les gestionnaires de la prestation des programmes et des services afin :
  - de veiller à ce que leurs besoins en matière de sécurité des TI soient comblés;
  - de leur prodiguer des conseils sur les mesures de protection;
  - de leur prodiguer des conseils sur les incidences éventuelles des menaces existantes et nouvelles;
  - de leur prodiguer des conseils sur le risque résiduel d'un programme ou d'un service;
- contrôler la conformité de l'Agence avec la présente norme et la documentation connexe;
- promouvoir la sécurité des TI au sein de l'Agence;
- établir un processus efficace de gestion des incidents liés à la sécurité des TI et en contrôler la conformité;
- examiner les profils de contrôle de sécurité de domaine et en recommander l'approbation;
- répondre aux demandes de l'ASM responsable des risques liés à la sécurité pour l'Agence et assurer la coordination du Programme de sécurité des TI de l'ASFC avec lui;
- coordonner les activités qui consistent à cerner les besoins en matière de sécurité des TI de l'Agence ainsi que ses contrôles de sécurité;
- coordonner la réalisation d'une évaluation de la sécurité des TI à l'échelle de l'Agence;
- aider les **gestionnaires responsables de la prestation des programmes et des services** (GPPS) à cerner les risques liés à la sécurité des systèmes d'information et formuler des recommandations pour atténuer les risques résiduels inacceptables;
- s'assurer que les risques liés à la sécurité des systèmes d'information sont évalués et que des recommandations d'atténuation sont transmises à l'ASM aux fins d'approbation;
- superviser le processus d'évaluation de la sécurité des TI de l'Agence (accréditation) et s'assurer qu'on satisfait aux exigences de l'ASFC en matière d'assurance de la sécurité des systèmes;
- communiquer et expliquer les menaces à l'échelle de l'Agence (telles que définies dans les évaluations de sécurité) aux différents secteurs opérationnels de l'ASFC.

**Coordonnateur de la planification de la continuité des activités (CPCA)**

- L'ASM est nommé CPCA. Le CPCA s'assure qu'on adopte une approche exhaustive en matière de protection de la capacité de l'Agence de fournir sans interruption les services essentiels aux Canadiens. À cette fin, le CPCO, en collaboration avec le DPI et le CSTI, peut utiliser le processus de gestion des risques liés à la sécurité des systèmes d'information de façon à garantir que les exigences touchant la sécurité des systèmes d'information et la continuité des opérations sont reflétées dans les besoins opérationnels de l'Agence en matière de sécurité et que ces exigences sont gérées adéquatement par les profils de contrôle de sécurité de domaine.

**Gestionnaires responsables de la prestation des programmes et des services (GPPS)/gestionnaires opérationnels**

Les GPPS/gestionnaires opérationnels sont les responsables désignés de l'ASFC en ce qui concerne les activités de leurs programmes et services respectifs. Les GPPS/gestionnaires opérationnels doivent s'assurer de maintenir un niveau de sécurité approprié dans le cadre de la prestation de leurs programmes et de leurs services et s'assurer qu'on intègre les exigences en matière de sécurité dans les plans opérationnels, les programmes, les services et les autres activités de gestion. Ils doivent travailler en collaboration avec les responsables de la sécurité de l'ASFC pour gérer, en permanence, les risques liés à leurs programmes et services. Les GPPS/gestionnaires opérationnels ont les responsabilités suivantes :

- déterminer les besoins opérationnels touchant la sécurité de leurs programmes et services et faire accréditer ces programmes et services grâce au processus d'accréditation de l'Agence déterminé par l'ASM et le CSTI;
- s'assurer que la sécurité des applications et des systèmes est évaluée (par le CSTI) avant leur mise en œuvre;
- travailler avec les spécialistes de la sécurité de l'Agence pour gérer les risques liés à la sécurité des TI;
- prendre des mesures correctives pour combler les déficiences cernées;
- s'assurer que les changements ou les modifications qu'on apporte à leurs systèmes ou applications sont évalués du point de vue de la sécurité (par le CSTI) au moyen du processus de gestion du changement;
- veiller au réexamen et à la réévaluation continue des risques liés à la sécurité des TI (par le CSTI).

**Autorisateurs**

L'autorisateur est le représentant de l'ASFC qui octroie une « autorisation » relativement à l'utilisation d'un système d'information. Le niveau de l'autorisateur doit correspondre au risque résiduel accepté et au niveau de responsabilité du programme appuyé et de sa prestation réussie. Dans la plupart des cas, l'autorisateur est le GPPS responsable du système opérationnel. Dans le cas des systèmes opérationnels critiques et majeurs, l'autorisateur peut être un cadre supérieur.

Les autorisateurs ont les responsabilités suivantes :

- recommander l'acceptation des risques résiduels à l'échelle de l'Agence comme défini dans le plan de sécurité ministériel;
- gérer les risques liés à la sécurité des TI dans leurs programmes et services et prendre des mesures pour atténuer de tels risques jusqu'à un niveau acceptable;
- accepter les mesures correctives décrites dans les plans d'action de la gestion pour améliorer le rendement associé au système;
- accorder (ou non) l'autorisation d'utiliser des systèmes d'information.

**Agents de sécurité des systèmes d'information (ASSI)**

Les ASSI sont responsables de la sécurité opérationnelle de leurs systèmes d'information respectifs, ce qui inclut la sélection, la mise en œuvre et le maintien de contrôles de sécurité liés à leur domaine de responsabilité de façon à s'assurer que les objectifs en matière de contrôle sont atteints. Parmi les responsabilités des ASSI, mentionnons les suivantes :

- aider à définir les besoins en matière de sécurité et de contrôle de sécurité de l'ASFC en faisant ce qui suit :
    - collaborer avec l'ASM et le CSTI pour définir la portée des activités de gestion des risques liés à la sécurité de l'Agence;
    - participer à la détermination des besoins opérationnels en matière de sécurité;
    - classer la sécurité des activités opérationnelles de l'ASFC;
    - contribuer à l'élaboration de profils de contrôle de sécurité de domaine de l'Agence;
- participer à la réalisation des évaluations de la menace à l'Agence;
- appuyer les activités d'évaluation de la sécurité et contribuer à l'élaboration du plan de sécurité ministérielle;
- s'assurer que la sélection des contrôles de sécurité répond aux besoins opérationnels en matière de sécurité;
- superviser le déploiement et l'application des contrôles de sécurité communs;

- superviser le déploiement et l'application des contrôles de sécurité liés à leur domaine de responsabilité;
- évaluer la mise en œuvre et l'efficacité des contrôles de sécurité, produire des rapports sur l'atteinte des objectifs en matière de contrôle dans le cadre des plans de sécurité des systèmes d'information et recommander des mesures correctives pour éliminer les déficiences cernées durant les activités de mesure du rendement et les évaluations;
- contrôler et évaluer le rendement des contrôles de sécurité mis en place (contrôles de sécurité communs et contrôles de sécurité liés précisément aux différents systèmes d'information);
- en partenariat avec le CSTI, fournir à l'ASM, aux gestionnaires à tous les niveaux et aux employés des conseils d'expert sur l'application et l'efficacité des contrôles de sécurité liés à leur domaine de responsabilité.

**Responsables du contrôle des services communs**

Un responsable du contrôle des services communs est un gestionnaire tiers responsable de la prestation de programmes ou de services qui met en œuvre et applique au nom de l'Agence un contrôle de sécurité lié à plusieurs systèmes d'information ou qui permet de soutenir plusieurs systèmes d'information. Les responsables du contrôle des services communs contribuent aux éléments suivants :

- le processus de gestion des risques liés à la sécurité des TI de l'ASFC;
- les évaluations de la menace de l'ASFC;
- l'élaboration des profils de contrôle de sécurité de domaine;
- la mise en œuvre et l'application des contrôles de sécurité communs.

**Architectes de sécurité d'entreprise**

Les architectes de sécurité d'entreprise doivent s'assurer que les exigences en matière de sécurité nécessaires pour protéger les activités opérationnelles de l'Agence sont prises en considération durant tout le cycle de vie du développement des systèmes et dans le cadre de gestion du cycle de vie des services. Ils doivent prodiguer des conseils et fournir une orientation à l'ASM, au coordonnateur de la sécurité de la TI, aux programmes et aux services et aux gestionnaires des opérations de TI sur un large éventail d'enjeux liés à la sécurité (p. ex. établir des limites pour les systèmes d'information, évaluer la gravité des faiblesses et des déficiences des systèmes d'information de l'Agence, les dispositions sur la sécurité des plans opérationnels, les approches d'atténuation des risques, les alertes de sécurité et les répercussions néfastes possibles des vulnérabilités cernées).

Les architectes de sécurité d'entreprise contribuent aux éléments suivants :

- les évaluations de la menace de l'ASFC;
- la spécification des objectifs de contrôle de la sécurité;
- l'élaboration des profils de contrôle de sécurité de domaine;
- la mise à jour des contrôles de sécurité.

**Gestionnaires des opérations de TI**

Les gestionnaires des opérations de TI ont les responsabilités suivantes :

- mettre en œuvre, utiliser, maintenir et éliminer un ou plusieurs systèmes d'information;
- appliquer les contrôles de sécurité communs;
- fournir des données sur le rendement des contrôles de sécurité appliqués dans les systèmes d'information dont ils assument la responsabilité opérationnelle.

**Gestionnaires de projet de TI**

Les gestionnaires de projet de TI ont les responsabilités suivantes :

- cerner les intervenants responsables de la sécurité et interagir avec eux;
- s'assurer que les exigences en matière de sécurité, y compris les politiques et les normes en matière de sécurité des TI, sont respectées dans le cadre des projets sur des systèmes de TI et les activités de conception ou de modification des systèmes d'information de l'Agence;
- intégrer les activités de gestion des risques liés à la sécurité des systèmes d'information et les produits livrables connexes dans les plans de projet.

**Employés**

Tous les cadres et les employés (permanents, nommés pour une période déterminée, occasionnels et à temps partiel) de l'ASFC, personnel contractuel, le personnel d'agence privée, les personnes en affectation ou en détachement (y compris les étudiants) et toute autre personne qui doit respecter les politiques de l'ASFC aux termes d'un contrat ou d'un protocole d'entente (PE) ont les responsabilités suivantes :

- protéger toute l'information et tous les actifs sous leur contrôle, sur les lieux de travail et à l'extérieur;
- appliquer des contrôles de sécurité relatifs à leur domaine de responsabilité pour s'assurer d'intégrer les exigences de sécurité aux processus, aux pratiques et à l'exécution des programmes quotidiens.

## 8 CONFORMITÉ ET RAPPORTS

L'ASFC doit assurer la bonne gestion de ses programmes et services. L'ASM et le CSTI doivent :

- contrôler activement les pratiques de gestion et les contrôles liés à la présente Directive;
- prendre des mesures correctives en cas de déficiences importantes ou lorsque des améliorations sont nécessaires;
- s'assurer que les mesures correctives sont communiquées à tous les employés concernés de l'ASFC.

## 9 CONSÉQUENCES

L'ASM est responsable de réaliser des enquêtes et de réagir aux rapports de non-conformité liés à la présente Directive et de s'assurer que des mesures correctives appropriées sont prises au besoin. Tout employé dont on détermine qu'il a violé les politiques, les directives ou les normes peut faire l'objet d'une nouvelle vérification de sécurité justifiée et d'une mesure disciplinaire, qui peut aller jusqu'au congédiement.

## 10 EXAMEN DE LA DIRECTIVE

La présente Directive sera examinée au moins tous les trois ans par le CSTI, le directeur général, Services d'infrastructure, Direction générale de l'information, des sciences et de la technologie (DGIST) et l'ASM.

## 11 RÉFÉRENCES

Politiques, directives, normes et lignes directrices connexes

**ASFC**

- Cadre de gestion du programme de sécurité de l'ASFC
- Politique sur l'utilisation des ressources électroniques
- Directive relative à la sécurité de l'environnement informatique

**Secrétariat du Conseil du Trésor**

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité ministérielle
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)

**Centre de sécurité des télécommunications Canada**

CSTC – ITSG 33 : Lignes directrices sur la gestion des risques liés à la sécurité des TI

## 12 DEMANDES DE RENSEIGNEMENTS

Veuillez adresser toute demande de renseignements au sujet de la présente directive à :

| |
|---|
| Direction générale de l'information, des sciences et de la technologie<br>**Coordonnateur de la sécurité de la TI, Sécurité et continuité des opérations des TI**<br>Courriel : CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca<br>Intranet : http://atlas/istb-dgist/services/it-ti-sec/it_ti_sec_eng.asp |
| Direction générale du contrôle<br>**Direction de la sécurité et des normes professionnelles**<br>Politique sur la sécurité, sensibilisation et coordination de programme<br>Courriel : Security-Policy_Politiques-sur-la-Securite@ASFC-asfc.gc.ca<br>Intranet : http://atlas/cb-dgc/sec/index_e.asp |

## DÉFINITIONS

Des définitions précises provenant de sources qui font autorité se trouvent dans le Lexique de la terminologie en sécurité.

Canada Border Services Agency | Agence des services frontaliers du Canada




Comptrollership Branch
Security and Professional Standards Directorate
Security Policy and Program Coordination Division

Information, Science and Technology Branch
Enterprise Services Directorate
IT Security and Continuity Division

# Canada Border Services Agency (CBSA) Information Technology (IT) Security Risk Management Directive

Version: 2.0

PROTECTION • SERVICE • INTEGRITY




# Table of Contents

Canada Border Services Agency | Agence des services frontaliers du Canada




# INFORMATION TECHNOLOGY (IT) SECURITY RISK MANAGEMENT DIRECTIVE

## 1 EFFECTIVE DATE

This directive is effective January 20, 2015.

## 2 DIRECTIVE

This directive replaces Chapter 20: Security Risk Management – Information Technology Threat and Risk Assessments and Chapter 21: Policy on Security Reviews and Inspections of Information Technology Systems of the CBSA Security Volume.

## 3 CONTEXT

The Policy on Government Security (PGS) states that the management of security requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving prevention, detection, response and recovery. The PGS also states that the management of security is most effective when it is systematically woven into the business, programs and culture of a department and the public service as a whole.

IT security risk management is an essential component of CBSA IT Security Program for ensuring the protection of CBSA business activities and information assets. Through the application of IT security risk management, Agency risks can be continuously monitored and assessed so that CBSA programs and services, and the information systems upon which they rely, operate within an acceptable level of risk.

CBSA's IT security risk management activities support CBSA's integrated risk management as these activities form a continuous, proactive, and systematic process to understand, manage, and communicate IT security risks from an organization-wide perspective.

To be fully effective, IT security risk management must be a continuous process of activities performed at all levels of a system or application life cycle.

## 4 APPLICATION

The IT security risk management directive applies to those responsible for the selection, development, implementation and maintenance of CBSA electronic resources comprised of IT networks, systems, applications and data.

Where the Agency electronically shares information or is interconnected with external organizations, the CBSA will collaboratively engage its partners, clients and key stakeholders in the application of this Directive as it pertains to their mutual working relationship and the continuous application of IT security risk management activities.




## 5 DIRECTIVE STATEMENT

Agency electronic services, resources, and information are protected through an effective IT Security Risk Management Framework.

### 5.1 OBJECTIVE

The objectives of the IT security risk management directive include:

a) Ensuring that IT security risk management is a continuous, integral part of all Agency activities that involve information systems;
b) Ensuring that all relevant stakeholders understand their associated roles and responsibilities as they relate to IT security risk management; and
c) Defining Agency IT security needs and security controls.

### 5.2 EXPECTED RESULTS

The expected results of this Directive are:

a) Risks related to the inappropriate use of Agency electronic services, resources and information are effectively mitigated and continuously managed;
b) An Agency-wide approach is taken to ensure the continuous assessment and monitoring of IT security risks to CBSA IT assets; and
c) IT security risk management is an identifiable and integral element of Agency management responsibility and accountability.

## 6 REQUIREMENTS

Effective IT Security Risk Management requires that:

a) Business needs for security are identified and documented;
b) Security controls are defined and assessed for common components (e.g. incident management, performance monitoring, identity management) in support of information systems;
c) The Agency leverages threat assessments to help ensure the implementation of information systems that address CBSA IT security requirements;
d) CBSA develop security control profiles tailored to CBSA business needs for security that IT projects can leverage when implementing and updating Agency information systems;
e) The performance of IT security controls implemented for the Agency is continuously monitored and assessed;
f) Vulnerabilities and weaknesses are identified; and
g) Corrective measures contained in the Management Action Plans (MAP) to ensure vulnerabilities and weaknesses are resolved, and to improve performance and the Agency's overall security posture are developed and implemented.

## 7 ROLES, RESPONSIBILITIES AND ACCOUNTABILITY

The management of security risks is most effectively accomplished with the involvement and collaboration of all stakeholders who are required to perform the duties outlined below.

**Chief Information Officer (CIO)**




The Vice-President (VP) ITSB has been appointed CIO. CIO responsibilities include:

- Ensuring a productive and functional relationship between the Departmental Security Officer (DSO) and IT Security Coordinator (ITSC) to foster a coordinated and comprehensive approach to the implementation of security program requirements;
- Ensuring appropriate security controls are applied to all Agency Information Management (IM) and IT assets, activities and processes; and
- Ensuring that the IT Security Coordinator provides periodic briefings to the CIO and the DSO regarding Enterprise IT security risks.

**Departmental Security Officer (DSO)**

The Director General (DG), Security and Professional Standards Directorate (SPSD), has been appointed DSO. The DSO develops, implements, monitors, and maintains a departmental security plan (DSP) and is responsible for managing the Agency security program. The DSO is responsible for:

- Formally accepting Agency-wide security risks;
- Incorporating business needs for security, Agency threat assessment results, Agency security control objectives and Agency security controls in the DSP for approval by the CBSA President (Deputy Head);
- Updating the DSP to reflect changes in business needs for security, security control objectives, and security control requirements;
- Overseeing the implementation of the proposed information systems security risk management activities; and
- With the assistance of ITSC, developing and promulgating the use of domain security control profiles for the implementation of Agency information systems for all IT CBSA projects.

**IT Security Coordinator (ITSC)**

The Director, IT Security and Continuity Division (ITSCD), is appointed IT Security Coordinator (ITSC). The ITSC must establish and manage an IT security function within the Agency security program and is responsible for:

- Establishing and managing the Agency IT security program as part of a coordinated departmental security program;
- Reviewing and recommending approval of departmental IT security policies and standards, and all policies that have IT security implications;
- Working closely with program and service delivery managers to:
  - ensure their IT security needs are met,
  - provide advice on safeguards,
  - provide advice on potential impacts of new and existing threats, and
  - provide advice on the residual risk of a program or service;
- Monitoring departmental compliance with this standard and associated documentation;
- Promoting IT security within the Agency;
- Establishing an effective process to manage IT security incidents, and monitor compliance with it;
- Reviewing and recommending approval of the domain security control profiles;
- Responding to and ensuring the coordination of the CBSA IT Security Program with the DSO who has responsibility for Agency security risks;

- Coordinating the activities of identifying Agency IT security needs and security controls;
- Coordinating the establishment of the Agency-wide IT security assessment;
- Assisting p**rogram and service delivery managers** (PSDMs) with identifying security risks to information systems and providing recommendations for mitigating unacceptable residual risks;
- Ensuring that security risks for information systems are assessed and recommendations for mitigation are referred to the DSO for approval;
- Overseeing the Agency IT security assessment process (certification) and ensuring that CBSA system security assurance requirements are met; and
- Communicating and explaining Agency-wide threats (as defined in security assessments) to CBSA business communities.

**Business Continuity Planning Coordinator (BCPC)**

- The DSO is appointed BCPC. The BCPC ensures a comprehensive approach to safeguarding the Agency's capacity to provide continuous essential services to Canadians. To that end, the BCPC, in collaboration with the CIO and the ITSC, can leverage the information system security risk management process to ensure that CBSA information systems security and business continuity requirements are reflected in Agency business needs for security, and that these requirements are adequately addressed by domain security control profiles.

**Program and Service Delivery Managers (PSDMs) / Business Managers**

PSDMs / Business Managers are designated CBSA authorities responsible for the operations of the respective programs and services. PSDMs / Business Managers must ensure an acceptable level of security for their programs and services and must ensure security requirements are integrated into business planning, programs, services, and other management activities. They must work with the CBSA security community to manage, on an ongoing basis, the risk to their programs and services. PSDMs / Business Managers are responsible for:

- Determining the business needs for the security of their programs and services and having those programs and services accredited through the Agency accreditation process as determined by the DSO and ITSC;
- Ensuring that the security of applications and systems is assessed (by ITSC) prior to implementation of those applications and systems;
- Working with Agency security specialists to risk manage the IT Security risks;
- Taking corrective action to address identified deficiencies;
- Ensuring that changes or modifications to be made to their systems or applications are security assessed (by ITSC) through the change management process; and
- Ensuring continuous reassessment and re-evaluation of IT Security risks (by ITSC)

**Authorizers**

The authorizer is the CBSA official who grants the "Authority to Operate" for an information system. The level of the authorizer must be commensurate with the residual risk being accepted and with the level of responsibility for the supported program and its successful delivery. In most cases, the authorizer is the PSDM in charge of the business system. For business critical and major systems the authorizer can be a more senior official.

The authorizers are responsible for:




- Recommending acceptance of Agency-wide residual risks as defined in the departmental security plan;
- Managing IT security risks for their programs and services, and taking action to mitigate such risks to an acceptable level;
- Accepting the corrective measures contained in the Management Action Plans to improve performance associated with the system; and
- Granting (or not) the Authority to Operate for information systems.

**Information System Security Officers (ISSOs)**

ISSOs are responsible for the operational security posture of their respective information systems which includes selecting, implementing and maintaining security controls related to their area of responsibility to ensure that control objectives are achieved. ISSOs responsibilities include:

- Assisting with the definition of CBSA security needs and security controls by:
  - Collaborating with DSO and ITSC in defining the scope of the Agency's security risk management activities,
  - Participating in the identification of business needs for security,
  - Categorizing the security of CBSA business activities, and
  - Contributing to the development of Agency domain security control profiles;
- Participating in conducting Agency threat assessments;
- Supporting security assessment activities and contributing to the development of the DSP;
- Ensuring that the selection of security controls satisfy business needs for security;
- Supervising the deployment and operation of common security controls;
- Supervising the implementation and operation of security controls related to their area of responsibility;
- Evaluating the implementation and effectiveness of security controls, reporting on the achievement of control objectives as part of information systems security plans, and recommending corrective action to address deficiencies identified in performance measurement and assessments;
- Monitoring and assessing the performance of implemented security controls (common security controls and information systems specific security controls); and
- In partnership with ITSC, providing the DSO, managers at all levels and employees with expert advice on the application and effectiveness of security controls related to their area of responsibility.

**Common Service Control Providers**

A common security control provider is a third-party program or service delivery manager who implements and operates a security control that is common to, or supports several information systems on behalf of the Agency. Common Service Control Providers contribute to:

- CBSA IT Security Risk Management process;
- CBSA threat assessments;
- Development of domain security control profiles; and
- Implementation and operation of common security controls.

**Enterprise Security Architects**

Enterprise Security Architects are responsible for ensuring that the security requirements necessary to protect the Agency's business activities are addressed throughout the system development life cycle and within the service life cycle management framework. Enterprise security architects should provide guidance and advice to the DSO, the IT security coordinator, programs and services, and IT operations managers on a range of security-related issues (e.g., establishing information system boundaries, assessing the severity of weaknesses and deficiencies in CBSA information systems, the security provisions of operations plans, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities).

Enterprise Security Architects contribute to:

- CBSA threat assessments;
- Specification of security control objectives;
- Development of domain security control profiles; and
- Updates to security controls.

**IT** Operations **Managers**

IT Operations Managers are responsible for:

- Implementing, operating, maintaining and disposing of one or more information systems;
- Operating common security controls; and
- Providing performance metrics for the security controls implemented in the information systems for which they have operational responsibility.

**IT Project Managers**

IT Project Managers are responsible for:

- Identifying and engaging security stakeholders;
- Ensuring that security requirements including IT security policy and standards are met in IT system projects and the design or changes to CBSA information systems; and
- Integrating information system security risk management activities and deliverables into their project plans.

**Employees**

All CBSA management and employees (permanent, term, casual, part-time), contract and private agency personnel, individuals seconded or assigned to CBSA (including students) and any other individuals required to comply with CBSA policies by virtue of a contract or a memorandum of understanding (MOU) are responsible for:

- Safeguarding all information and assets under their control both onsite and offsite; and
- Applying security controls related to their area of responsibility to ensure that security requirements are integrated into day-to-day processes, practices and program delivery.

## 8 COMPLIANCE AND REPORTING

CBSA is responsible for ensuring that its programs and services are well managed. The DSO and the ITSC must:

- Actively monitor management practices and controls related to this Directive;

- Take remedial action where significant deficiencies are encountered or improvements are needed; and
- Ensure that remedial actions are communicated to all relevant CBSA staff.

## 9 CONSEQUENCES

The DSO is responsible for investigating and responding to reports of non-compliance with this Directive and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies, directives, or standards, may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment.

## 10 DIRECTIVE REVIEW

This Directive shall be reviewed at least every three years by the ITSC, the Director General of Infrastructure Services, Information, Science and Technology Branch (ISTB), and the DSO.

## 11 REFERENCES

Related Policies, Directives Standards and Guidelines:

**CBSA**

- CBSA Security Program Management Framework
- Policy on the Use of Electronic Resources Policy
- Directive for the Security of the Computing Environment

**Treasury Board Secretariat**

- Policy on Government Security
- Directive on Departmental Security Management
- Operational Security Standard: Management of IT Security (MITS)

**Communications Security Establishment Canada**

CSEC – ITSG 33: IT Security Risk Management Guidelines

## 12 ENQUIRIES

Enquiries regarding this directive should be directed to:

| |
|---|
| Information, Science and Technology Branch,<br>**IT Security Coordinator, IT Security and Continuity Division**<br>E-mail: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca<br>Intranet: http://atlas/istb-dgist/services/it-ti-sec/it_ti_sec_eng.asp |

Comptrollership Branch,
**Security and Professional Standards Directorate**
Security Policy, Awareness, and Program Coordination
E-mail: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca
Intranet : http://atlas/cb-dgc/sec/index_e.asp

## DEFINITIONS

Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Standard for CBSA Audit Trails for Information Systems

**Abstract**

This document establishes the standard for audit trails management for information systems, in support of audit and accountability.

PROTECTION • SERVICE • INTEGRITY

Canada

# Table of Contents

# 1. Effective Date

This standard is effective June 1, 2016.

# 2. Context

The Operational Security Standard: Management of Information Technology Security (MITS) specifies that, at a minimum, departments must include a security audit function in all information systems, as part of their ability to detect and prevent unauthorized activities.

This requirement supports the proactive detection and after-the-fact investigation of suspected employee wrong-doing, and specifically via the unauthorized use of information employees have access to in order to perform their duty.

# 3. Application

This standard applies to all individuals responsible for the selection, development, implementation and maintenance of CBSA electronic resources that is comprised of IT networks, systems, applications and data. These individuals include the program and service delivery managers (owners of systems and applications) and all technical personnel, CBSA and service provider employees (technical resources responsible for systems and applications development and maintenance).

Where the Agency electronically shares information or is interconnected with external organizations, the CBSA will collaboratively engage its partners, clients and key stakeholders in the application of this standard as it pertains to their mutual working relationship.

Any project planning a new information system or major changes to a legacy information system must adhere to this standard.

Managers of service provider contracts (e.g. external vendors, SSC) must also ensure that service providers meet the requirements of this standard.

# 4. Standard Statement

This standard supports the Directive on IT Security Risk Management.

### 4.1. Objective

The objective of this standard is to deter and detect the unauthorized use of CBSA information and information systems. In addition, this standard will support individual accountability, reconstruction of events and investigations.

### 4.2. Expected Results

The expected results of this standard are:

- Enhanced deterrence of unauthorized use of CBSA information and information systems
- Increased ability of programs and services to define business risk, inappropriate use of information systems and suspicious activities;
- Increased ability to define, capture, secure and manage audit records;
- Enhanced pro-active response to business risk;
- Improved investigations of potential unauthorized use of CBSA information and information systems; and
- Adoption of the Central Audit Trails Management System (CATMS) to provide an Agency-wide consistent management of audit trails.

# 5. Requirements

### 5.1. Process Overview

The following high-level process must be followed by any project planning a new information system or major changes to a legacy information system – in collaboration and consultation with the CBSA Departmental Security Officer (DSO):

| | |
|---|---|
| 1 | Define audit trails to be captured, applying DSO's risk based methodology to all data elements of the information system |
| 2 | Determination on use of Central Audit Trails Management System (when available) |
| 3 | Detailed definition of audit trails management function (format, capture, transport, storage) |
| 4 | Implementation of audit trails management function as part of the information system implementation |
| 5 | Testing of audit trails management function (validation that audit trails are properly captured, transported, stored and available for analysis) |

## 5.2. Audit Trails Definition and Generation

### 5.2.1. Auditable Events

The DSO representatives and the information system business owner perform a risk assessment of the information system and its business context.

Jointly they perform a risk-based analysis of the data elements and actions (e.g. read, add, delete, disable, print, save, export, etc.) and they define the list of events that the information system must be capable of auditing and provide a rationale for why this list is deemed to be adequate to support pro-active and after-the-fact investigations of security incidents.

All actions on data elements containing personal information must be included in the list of auditable events, including a copy of all information that was accessed by a user (in whole or in part) as a result of the action executed by this user at the point in time it was accessed (e.g., copy of report generated, copy of query result displayed on screen, copy of tombstone data viewed, copy of enforcement data viewed, copy of work item content viewed).

The list of auditable events must include the execution of privileged functions (e.g. admin rights). This is one way to prevent misuse of privileged functions, intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised CBSA accounts.

The DSO representatives also ensures that adequate coordination with other organizational entities requiring audit-related information is established, in order to enhance mutual support and to help guide the selection of auditable events.

### 5.2.2. Review of Auditable Events

The DSO representatives and the information system owner review the list of auditable events on an annual basis, or more frequently if required.

### 5.2.3. Content of Audit Records

The information system produces audit records that contain sufficient information to, at a minimum, establish the following:

Standardized Content of Audit Records

| |
|---|
| 1. **Type of event** – e.g. authorize, create, read, update, delete. |
| 2. **Identity of any user/subject associated with the event** – e.g. process or transaction name, process or transaction identifier |
| 3. **Source of the event** (as many as available) for the subject requesting the action – e.g. user name, computer name, IP address, and MAC address, physical location. |
| 4. **Outcome of the event** – e.g. success or failure of the action |
| 5. **Date and timestamp** of the event (Note: the time stamping section of this standard |

| |
|---|
| includes requirements regarding time source and time format). |
| 6. **Event description** – A description with as much detail as available depending upon individual systems and as required (for instance full-text recording of privileged commands) |
| 7. **Event severity** – Systems must classify and record event severity. Classification schemas and severity levels must be sufficiently described. |

#### 5.2.4. Permitted Actions

The information system specifies the permitted actions for each process, role, and/or user. Permitted actions are detailed in the information system documentation (for instance read, write, append and delete).

#### 5.2.5. Audit Generation

The information system enables the selection of which auditable events are to be audited. It also generates audit records for the list of selected auditable events and with the content defined by the information system owner and the DSO representatives.

#### 5.2.6. Identification and Authentication

The information system must comply with CBSA's identification and authentication requirements to ensure the exact attribution of audit records to information system users.

### *5.3. Audit Trails Management Infrastructure*

#### 5.3.1. Central Audit Trails Management System

When possible, information systems must transfer audit records, in a timely and secure manner, to the Central Audit Trails Management System (CATMS). A centralized system is better suited to protect audit records. Audit records transferred to CATMS can be deleted from the information system.

#### 5.3.2. Centralization

When required by the categorization of the information system, audit records must be centralized, in a standardized format, to facilitate the review and analysis from multiple components within the information system.

#### 5.3.3. Audit Record Storage Capacity

The information system allocates audit record storage capacity to reduce the likelihood of such capacity being exceeded. Considerations must be given to audit storage within the information system as well as within CATMS storage (if it is used).

### 5.3.4. Insufficient Audit Storage Capacity Alerting

The information system must also provide a warning when audit record storage has reached:

- 75% of maximum audit storage capacity, or
- Another level - defined in the information system documentation, depending on actual storage provisioned and on growth rate of audit records storage.

### 5.3.5. Response to Audit Processing Failures

Actions to take in the event of an audit processing failure must be defined in advance. Taken actions include:

- Alerting of designated officials (captured in a list including name, function and emergency contact information).
- Remediation or mitigation actions (e.g. shutdown of the information system operation without or with degraded audit records logging capabilities, overwrite of old audit records to save newer ones, loss of newer audit records).

### 5.3.6. Time Stamping

The information system uses internal system clocks, synchronized on a daily basis (minimum required standard) to a trusted time source, to generate time stamps for audit records.

### 5.3.7. Protection of Audit Records

The information system protects audit records and audit tools from any unauthorized access, modification and deletion. Transferring audit records to CATMS ensures such protection, but audit records must still be protected before and during transfer.

Access to the management of audit functionality is authorized to a limited subset of privileged users, as defined in the information system documentation and in CATMS documentation.

Special consideration must be given to any non-local access (e.g. remote access) to privileged accounts and to any execution of privileged functions on CATMS, in order to ensure the confidentiality, integrity and availability of audit records.

### 5.3.8. Audit Records Backup

The information system backs up audit records onto a different system or media than the system being audited. Backups retention follows CBSA operational procedures and must also comply with section 5.3.9 below.

### 5.3.9. Retention and Disposition

Audit records must be retained and disposed according to CBSA information management policies, and specifically Government of Canada multi institution disposition authorities (MIDAs) and CBSA institution-specific disposition authorities (ISDAs)[1].

## 5.4. Review, Analysis and Reporting

### 5.4.1. Request

A request for an audit trail report is made:

- In response to a complaint,
- In support of an investigation into allegations or suspicion of unauthorized access, or
- In response to an Access to Information Privacy (ATIP) Act.

The request for an audit trail is designated as Protected B information as defined by the CBSA Policy on Information Security. It is also considered personal information as defined by the Privacy Act. Consequently the communication of the request, the audit trails report, and results of its analysis must be restricted to individuals with "a need to know".

The DSO representative from the Security and Professional Standard Directorate is the functional authority for the CATMS and provides advice and guidance along with analysis expertise when required.

A request to access audit trails for review, analysis and reporting must be submitted to the Director, Infrastructure and Information Security Division via a generic mailbox. The request can be sent by encrypted email and should include a brief explanation of the reason for the request, the user's name and User ID and/or any information available that would assist in reviewing the request. DSO representatives will coordinate with the requester to provide the requested information in a secure manner, to assist requesters or to explain why a request cannot be granted.

### 5.4.2. Review

Information system audit records must be reviewed and analyzed, according to their severity.

**Sample Application Event Severity Classification**

| Numerical Code | Severity |
|---|---|
| A | Urgent: event requires immediate alerting |
| B | Important: event may require later review |
| C | Standard: event to be logged without further action |

Audit records review, analysis, and reporting processes must be integrated to support organizational processes for investigation and response to suspicious activities.

### 5.4.3. Adjustable Level of Review

The Agency adjusts the level of audit review, analysis and reporting within the information system when there is a change in risk to:

- Organizational operations,
- Organizational assets,
- Individuals,
- Other organizations, or
- Canada, based on law enforcement information, intelligence information, or other credible sources of information.

The DSO representatives coordinate such adjustments with the information system business owners.

### 5.4.4. Situational Awareness

When required by the information system security requirements, the Agency analyzes and correlates audit records across different information systems to gain CBSA-wide situational awareness. Such a requirement, as determined by the information system owner and the DSO, applies to sensitive systems (e.g. Classified Secret) and is documented in the information system security plan.

### 5.4.5. Audit Reduction and Report Generation

When required the information system must provide an audit reduction and report generation capability, that is to say support for near real-time audit review, analysis and reporting and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. CATMS provides such a capability. Such a requirement, as determined by the information system owner and the DSO, is based on the analysis of the business needs for security and is documented in the information system security plan.

Furthermore, the information system must provide the capability to automatically process audit records for events of interest based on selectable event criteria.

### 5.4.6. Shared Services Canada (SSC)

Audit trails information captured by Shared Services Canada will be leveraged in support of CBSA investigations and correlated with the audit trails information captured by CSBA, as required by this standard.

# 6. Roles and Responsibilities

The following table represents roles and responsibilities associated with audit trails.

Legend:

- A for Accountable: Represents the role ultimately answerable for the correct and thorough completion of the task, and the one who delegates the work to those responsible. There is one and only one Accountable per task.
- R for Responsible: Represents the role(s) that do the work to achieve the task. There is at least one Responsible per task.
- C for Consulted: Represents the role(s) whose opinions are sought, typically subject matter experts, and with whom there is two-way communication.

Roles:

- PSDM: Program and/or Service Delivery Manager
- DSO: Departmental Security Officer (Director General, SPSD)
- ITSC: IT Security Coordinator (Director, ITSCD)
- ISTB: Information, Science and Technology Branch – including Liaison with SSC and CRA
- IM: Information Management

| | **PSDM** | **DSO** | **ITSC** | **ISTB** | **IM** |
|---|---|---|---|---|---|
| ***Information System Audit Trails*** | | | | | |
| Define and review auditable events | A+R | R | C | | |
| Define content of audit records | A+R | R | C | | |
| Define permitted actions | A+R | C | C | | |
| Validate audit generation capabilities | A+R | R | C | | |
| Maintain audit records storage capacity | A+R | C | C | R | |
| Define response to audit processing failures | A+R | R | C | C | |

| | PSDM | DSO | ITSC | ISTB | IM |
|---|---|---|---|---|---|
| Time stamping of audit trails | A+R | C | C | R | |
| Protection of audit records in information system | A+R | C | C | C | |
| Backup audit records | A+R | C | C | R | |
| Define retention and disposition | A+R | R | C | | R |
| ***CBSA Enterprise Capability***[2] | | | | | |
| Protection of audit records in CATMS | | A+R | | R | |
| Centralize audit trails in CATMS | R | A+R | C | C | |
| Provide audit reduction and report generation capabilities in CATMS | C | A+R | | C | |
| Provide time synchronization | | C | | A+R | |
| Review audit logs and respond | C | A+R | C | C | |
| Manage adjustments of level of review | R | A+R | C | R | |
| Provide situational awareness reports | C | A+R | C | C | |

[2] The DSO is the business owner in charge of the Central Audit Trails Management System in order to ensure adequate and secure collection, management and review of audit logs. ISTB is the technical owner in charge of technical operations.

# 7. Compliance and Reporting

The CBSA Departmental Security Officer, the IT Security Coordinator, security practitioners and managers are responsible for monitoring compliance with this standard within CBSA, and for measuring the effectiveness of audit trails management.

Employees will report security incidents in accordance with the requirements outlined in the CBSA Security Volume, Security Incident Reporting.

# 8. Consequences

The DSO is responsible for investigating and responding to reports of non-compliance with this standard and ensuring that appropriate remedial actions are taken when/as required. Any employee found to have violated policies, directives or standards may be subject to security screening review for cause as well as disciplinary action, up to and including termination of employment.

# 9. Standard Review

This standard shall be reviewed every three years or more frequently as directed by the ITSC and the DSO.

# 10. Definitions

| Term | Definition |
|---|---|
| Audit Record | The formal record of an IT event. |
| Audit Trails Management | The process for generating, transmitting, storing, analyzing, and disposing of audit records. |
| Event | In the case of Information Technology (IT) systems, an occurrence within an information system (at the infrastructure or application layer). |

# 11. References

## 11.1. CBSA

- Directive for IT Security Risk Management

## 11.2. Treasury Board Secretariat

- Policy on Government Security
- Policy Framework for Information and Technology
- Policy on Access to Information
- Policy on Internal Audit
- Policy on Management of Information Technology
- Policy on Privacy Protection
- Directive on Recordkeeping
- Operational Security Standard: Management of IT Security (MITS)

## 11.3. Communications Security Establishment Canada

- CSEC – ITSG 33: IT Security Risk Management

## 11.4. Enquiries

Advice on this Standard can be obtained from:

IT Security & Continuity Division
Enterprise Services Directorate
Information Science and Technology Branch
CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca

and/or

Information & Infrastructure Security Division
Security and Professional Standards Directorate
Comptrollership Branch
Information_Security-Securite_de_linformation@cbsa-asfc.gc.ca

Agence des services frontaliers du Canada | Canada Border Services Agency



# Norme relative aux pistes de vérification de l'ASFC pour les systèmes d'information

**Résumé**

Le présent document établit la norme de gestion des pistes de vérification pour les systèmes d'information à l'appui des vérifications et de l'obligation de rendre compte.

PROTECTION • SERVICE • INTÉGRITÉ

Canada

---

**Table des matières**

# 1. Date d'entrée en vigueur

La présente norme entre en vigueur le 1er juin 2016.

# 2. Contexte

La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) précise qu'au minimum, les ministères doivent inclure une fonction de vérification de la sécurité dans tous les systèmes d'information, ce qui améliore leur capacité de détecter et de prévenir les activités non autorisées.

Cette exigence appuie la détection proactive, et l'enquête après coup, des actes répréhensibles soupçonnés de la part d'employés, plus précisément par l'utilisation non autorisée des renseignements auxquels les employés ont accès afin d'accomplir leurs tâches.

# 3. Application

Cette norme s'applique à toutes les personnes responsables de la sélection, de l'élaboration, de la mise en œuvre et du maintien des ressources électroniques de l'Agence des services frontaliers du Canada (ASFC), à savoir les réseaux, les systèmes, les applications et les données de technologie de l'information (TI). Ces personnes comprennent les gestionnaires d'exécution des programmes et de prestation des services (responsables des systèmes et des applications), tout le personnel technique, les employés de l'ASFC et du fournisseur de services (ressources techniques chargées de l'élaboration et du maintien des systèmes et des applications).

Dans les cas où l'Agence communique des renseignements de façon électronique ou est interconnectée à des organisations externes, l'ASFC collabore avec ses partenaires, ses clients et les intervenants clés en vue d'appliquer cette norme en fonction de leur relation de travail mutuelle.

Tout projet prévoyant un nouveau système d'information ou des changements importants à un ancien système d'information doit respecter cette norme.

Les gestionnaires des marchés conclus avec les fournisseurs de service (p. ex., les fournisseurs externes et Services partagés Canada [SPC]) doivent également s'assurer que les fournisseurs de service satisfont aux exigences de la norme.

# 4. Énoncé de la norme

La présente norme appuie la Directive sur la gestion du risque en matière de sécurité des TI.

## 4.1. Objectif

La présente norme vise à dissuader et détecter l'utilisation non autorisée de l'information et des systèmes d'information de l'ASFC. De plus, cette norme contribue à renforcer l'obligation personnelle de rendre compte, la reconstitution des évènements et les enquêtes.

## 4.2. Résultats prévus

La présente norme vise l'atteinte des résultats suivants :

- Amélioration de la dissuasion de l'usage non autorisé de l'information et des systèmes d'information de l'ASFC;
- Amélioration de la capacité des programmes et des services de définir les risques opérationnels, l'utilisation inappropriée des systèmes d'information et les activités suspectes;
- Amélioration de la capacité de définir, d'enregistrer, d'entreposer de façon sécuritaire et de gérer les dossiers de vérification;
- Amélioration de l'intervention proactive par rapport aux risques opérationnels;
- Amélioration des enquêtes relatives à l'utilisation potentiellement non autorisée de l'information et des systèmes d'information de l'ASFC;
- Adoption du Système central de gestion des pistes de vérification (SCGPV) en vue de permettre une gestion cohérente des pistes de vérification à l'échelle de l'Agence.

# 5. Exigences

## 5.1. Aperçu du processus

Le processus général suivant doit être suivi par tout projet prévoyant un nouveau système d'information ou des changements importants à un ancien système d'information, en collaboration et en consultation avec l'agent de sécurité ministériel (ASM) de l'ASFC :

| | |
|---|---|
| 1 | Définition des pistes de vérification à enregistrer en appliquant la méthode axée sur le risque de l'ASM à tous les éléments de données du système d'information. |
| 2 | Détermination de l'utilisation du Système central de gestion des pistes de vérification (quand il sera disponible). |
| 3 | Définition détaillée de la fonction de gestion des pistes de vérification (format, enregistrement, transport et entreposage). |
| 4 | Mise en œuvre de la fonction de gestion des pistes de vérification |

| | |
|---|---|
| | dans le cadre de la mise en œuvre du système d'information. |
| 5 | Mise à l'essai de la fonction de gestion des pistes de vérification (confirmation que les pistes de vérification sont bien enregistrées, transportées et entreposées et sont disponibles aux fins d'analyse). |

## *5.2. Définition et création de pistes de vérification*

### 5.2.1. Évènements vérifiables

Les représentants de l'ASM et le responsable opérationnel du système d'information effectuent une évaluation des risques du système d'information et de son contexte opérationnel.

Ensemble, ils effectuent une analyse fondée sur les risques des éléments de données et des actions (p. ex., lire, ajouter, supprimer, désactiver, imprimer, enregistrer, exporter, etc.) et ils définissent la liste des évènements que le système d'information doit pouvoir vérifier. De plus, ils expliquent pourquoi la liste est considérée comme étant adéquate pour appuyer les enquêtes proactives et après coup sur les incidents relatifs à la sécurité.

Toutes les actions liées aux éléments de données qui contiennent des renseignements personnels doivent figurer sur la liste d'évènements vérifiables, ainsi qu'une copie de tous les renseignements consultés par un utilisateur (en totalité ou en partie) à la suite de l'action prise par ce dernier au moment où les renseignements ont été consultés (p. ex., une copie du rapport produit, une copie des résultats de la recherche affichés à l'écran, une copie des renseignements de base consultés, une copie des données sur l'exécution de la loi et une copie du contenu de la tâche consultée).

La liste des évènements vérifiables doit comprendre l'exécution de fonctions privilégiées (e.g. droits administratifs). Ceci est une méthode pour empêcher l'utilisation non approuvée des fonctions privilégiées par des utilisateurs non approuvés, ou par des organismes externes non autorisés qui ont compromis des comptes de l'ASFC.

Les représentants de l'ASM doivent également veiller à ce qu'une coordination adéquate soit établie avec d'autres entités organisationnelles devant obtenir des renseignements liés aux vérifications afin d'améliorer le soutien mutuel et d'orienter la sélection d'évènements vérifiables.

### 5.2.2. Examen des évènements vérifiables

Les représentants de l'ASM et le responsable du système d'information examinent la liste des évènements vérifiables chaque année ou plus fréquemment au besoin.

### 5.2.3. Contenu des dossiers de vérification

Le système d'information produit des dossiers de vérification qui contiennent suffisamment d'information pour, à tout le moins, établir ce qui suit :

Contenu normalisé des dossiers de vérification

| |
|---|
| 1. **Type d'événement –** P. ex., autoriser, créer, lire, mettre à jour ou supprimer. |
| 2. **Identité de tout utilisateur ou sujet associé à l'événement –** P. ex., nom du processus ou de la transaction et identificateur du processus ou de la transaction. |
| 3. **Source de l'événement** (le plus grand nombre possible) pour le sujet qui demande l'action – P. ex., nom de l'utilisateur, nom de l'ordinateur, adresse IP, adresse MAC et emplacement matériel. |
| 4. **Résultat de l'événement –** P. ex., réussite ou échec de l'action. |
| 5. **Date et heure système** de l'événement (Nota : La partie sur l'heure système de la présente norme comprend des exigences en matière de source horaire et de format de l'heure.) |
| 6. **Description de l'événement –** Une description qui contient le plus de renseignements possible en fonction des systèmes individuels et des besoins (p. ex., enregistrement contenant le texte intégral des commandes privilégiées). |
| 7. **Gravité de l'événement –** Les systèmes doivent classer et enregistrer la gravité de l'événement. Les schémas de classification et les niveaux de gravité doivent être décrits adéquatement. |

### 5.2.4. Actions permises

Le système d'information précise les actions permises pour chaque processus, rôle et/ou utilisateur autorisé du système d'information. Les actions permises sont détaillées dans la documentation du système d'information (p. ex., lire, écrire, annexer et supprimer).

### 5.2.5. Production des dossiers de vérification

Le système d'information permet de sélectionner quels évènements vérifiables seront vérifiés. Il produit également les dossiers de vérification pour la liste d'évènements vérifiables, qui comprennent le contenu défini par le responsable du système d'information et les représentants de l'ASM.

### 5.2.6. Identification et Authentification

Le système d'information doit répondre aux exigences de l'ASFC en matière d'identification et d'authentification pour s'assurer de l'attribution exacte des dossiers de vérification aux utilisateurs du système d'information.

## *5.3. Infrastructure de gestion des pistes de vérification*

### 5.3.1. Système central de gestion des pistes de vérification

Dans la mesure du possible, les systèmes d'information doivent transférer les dossiers de vérification de façon sécuritaire et en temps opportun au Système central de gestion des pistes de vérification (SCGPV). Un système central est plus à même de protéger les dossiers de vérification. Les dossiers de vérification transférés au SCGPV peuvent être effacés des systèmes d'information.

### 5.3.2. Centralisation

Lorsque la classification du système d'information l'exige, les dossiers de vérification doivent être centralisés, en fonction d'un modèle normalisé, afin de faciliter l'examen et l'analyse par de multiples composants du système d'information.

### 5.3.3. Capacité de stockage des dossiers de vérification

Le système d'information attribue une capacité de stockage des dossiers de vérification afin de réduire la probabilité que cette capacité soit dépassée. Il faut prendre en considération la possibilité de stocker des dossiers de vérification dans le système d'information ainsi que dans le SCGPV (s'il est utilisé).

### 5.3.4. Alerte de capacité de stockage des dossiers de vérification insuffisante

Le système d'information doit également donner un avertissement lorsque le volume de stockage des dossiers de vérification attribué atteint:

- 75 % de la capacité maximale de stockage, ou
- Un autre pourcentage tel qu'il est défini dans la documentation du système d'information (en fonction de la capacité de stockage réelle fournie et du taux de croissance du stockage des dossiers de vérification).

### 5.3.5. Interventions en cas d'échec de vérification

Des mesures sont définies aux fins d'intervention en cas d'échec de vérification du système d'information. Les mesures définies incluent:

- Alerte des représentants désignés (une liste est dressée, qui contient leur nom, leur fonction et leurs coordonnées en cas d'urgence).
- Mesures correctrices ou d'atténuation (p. ex., l'arrêt de l'utilisation du système d'information avec ou sans des capacités réduites de journalisation des dossiers de vérification, le remplacement d'anciens dossiers de vérification afin d'enregistrer des dossiers plus récents, la perte de nouveaux dossiers de vérification).

### 5.3.6. Inscription de l'heure système

Le système d'information utilise ses horloges internes, qui sont synchronisées au moins une fois par jour (standard minimum) avec une source fiable, pour générer l'horodatage des dossiers de vérification.

### 5.3.7. Protection des dossiers de vérification

Le système d'information protège les dossiers de vérification et les outils de vérification contre les accès non autorisés, les modifications et la suppression. Le transfert des dossiers de vérification au SCGPV permet d'assurer cette protection, mais les dossiers de vérification doivent encore être protégés avant et pendant le transfert.

L'accès aux fonctions de gestion de la vérification est uniquement autorisé à un sous-ensemble limité d'utilisateurs privilégiés, tel qu'il est défini dans la documentation du système d'information et dans celle du SCGPV.

Des considérations particulières doivent également être données à l'accès à distance aux comptes privilégiés et à l'exécution des fonctions privilégiées du SCGPV, afin d'assurer la confidentialité, l'intégrité et la disponibilité des dossiers de vérification.

### 5.3.8. Sauvegarde des dossiers de vérification

Le système d'information sauvegarde les dossiers de vérification dans un autre système ou support que celui qui fait l'objet d'une vérification. La conservation des sauvegardes suit les procédures opérationnelles de l'ASFC et doit aussi se conformer à la section 5.3.9 ci-après.

### 5.3.9. Conservation et élimination

Les dossiers de vérification doivent être conservés et éliminés conformément aux politiques de gestion de l'information de l'ASFC, et plus particulièrement aux autorisations pluri-institutionnelles de disposer des documents (APDD) du gouvernement du Canada et les autorisations spécifiques de disposer de documents (ASDD) de l'ASFC[1].

## *5.4. Examen, analyse et établissement de rapports*

### 5.4.1. Demande

Une demande de rapport de piste de vérification est présentée:

---

- à la suite d'une plainte,
- à l'appui d'une enquête sur des allégations ou des soupçons d'accès non autorisé, ou
- en réponse à une demande d'accès à l'information en vertu de la *Loi sur l'accès à l'information et sur la protection des renseignements personnels*.

Une demande est considérée étant des renseignements « Protégé B », tel qu'il est défini dans la Politique sur la sécurité de l'information de l'ASFC. Elle est aussi considérée comme étant des renseignements personnels, tel qu'il est défini dans la *Loi sur la protection des renseignements personnels*. Par conséquent, l'accès à la communication de la demande, au rapport de piste de vérification et aux résultats de son analyse doit être limité aux personnes qui ont « un besoin de savoir ».

Le représentant de l'ASM de la Direction de la sécurité et des normes professionnelles (DSNP) est l'autorité fonctionnelle pour le SCGPV, et il donne des conseils et une orientation, ainsi qu'une expertise en matière d'analyse, au besoin.

Une demande d'accès aux pistes de vérification aux fins d'examen, d'analyse et d'établissement de rapports doit être présentée au directeur de la Division de l'infrastructure et de la sécurité de l'information par l'intermédiaire d'une boîte de courriel générique. La demande, qui peut être envoyée par courriel chiffré, doit expliquer brièvement la raison de la demande et comprendre le nom de l'utilisateur et son ID utilisateur, ainsi que tout autre renseignement qui faciliterait l'examen de la demande. Les représentants de l'ASM collaboreront avec les demandeurs afin de fournir les renseignements demandés de façon sécuritaire, d'aider les demandeurs ou d'expliquer pourquoi une demande a été rejetée.

### 5.4.2. Examen

Les dossiers de vérification du système d'information doivent être examinés et analysés en fonction de leur gravité.

**Modèle de classification de la gravité d'un évènement survenu dans une application**

| Code numérique | Gravité |
|---|---|
| A | Urgent : L'évènement nécessite une alerte immédiate, |
| B | Important : L'évènement pourrait faire l'objet d'un examen ultérieur. |
| C | Ordinaire : L'évènement doit être consigné sans prendre aucune action supplémentaire. |

L'examen des dossiers de vérification, l'analyse et les rapports de vérification doivent être intégrés pour appuyer les processus organisationnels d'enquête et d'intervention relatifs aux activités suspectes.

### 5.4.3. Quantité d'examens réglable

L'Agence adapte le niveau des vérifications, des analyses et des rapports pour un système d'information en cas de changements relatifs aux risques liés:

- aux activités organisationnelles,
- aux actifs de l'organisation,
- aux personnes
- aux autres organisations, ou
- au Canada, selon l'information des services d'exécution de la loi, du renseignement ou d'autres sources de renseignements crédibles.

Les représentants de l'ASM coordonnent ces réglages avec les responsables opérationnels des systèmes d'information.

### 5.4.4. Connaissance de la situation

Lorsque c'est requis par les exigences de sécurité d'un système d'information, l'Agence analyse et met en corrélation les dossiers de vérification de divers systèmes d'information pour acquérir une connaissance de la situation à l'échelle de l'ASFC. Un tel prérequis, déterminé par le gestionnaire du système d'information et l'ASM, s'applique aux systèmes sensibles (p. ex., Classifié Secret) et est documenté dans le plan de sécurité du système d'information.

### 5.4.5. Réduction des vérifications et établissement de rapports

Lorsque c'est requis par les exigences de sécurité d'un système d'information, le système d'information doit fournir une capacité de réduction des vérifications et d'établissement de rapports, c'est-à-dire un soutien pour l'examen, l'analyse et l'établissement de rapports de vérification en temps quasi réel et les enquêtes après coup sur les incidents relatifs à la sécurité. Les outils de réduction des vérifications et d'établissement de rapports ne modifient pas les dossiers de vérification originaux, mais le SCGPV offre cette capacité. Un tel prérequis, déterminé par le gestionnaire du système d'information et l'ASM, est basé sur l'analyse des besoins d'affaires en sécurité et est documenté dans le plan de sécurité du système d'information.

De plus, le système d'information doit fournir une capacité de traitement automatique des dossiers de vérification fondée sur des critères de sélection d'évènements pour les évènements d'intérêt.

### 5.4.6. Services partagés Canada (SPC)

Les renseignements sur les pistes de vérification enregistrés par Services partagés Canada appuieront les enquêtes de l'ASFC et seront mis en corrélation avec les renseignements sur les pistes de vérification enregistrés par l'ASFC conformément aux exigences de la présente norme.

# 6. Rôles et responsabilités

Le tableau ci-dessous présente les rôles et les responsabilités associés aux pistes de vérification.

Légende

- « A » correspond à « autorité » : La personne qui doit rendre compte de l'exécution exacte et méticuleuse de la tâche et celle qui délègue les tâches aux personnes responsables. Il n'y a qu'une autorité par tâche.
- « R » correspond à « responsable » : Les personnes qui sont chargées d'effectuer les travaux pour réaliser la tâche. Il y a au moins un responsable par tâche.
- « C » correspond à « consulté » : Les personnes que l'on consulte pour obtenir leur avis. Il s'agit souvent d'experts en la matière, avec qui l'on entretient une communication bilatérale.

Rôles:

- CGEPPS : Gestionnaire de l'exécution des programmes et de la prestation des services
- ASM : Agent de sécurité ministériel (directeur général, Direction de la sécurité et des normes professionnelles [DSNP])
- CSTI : Coordonnateur de la sécurité de la TI (directeur, Division de la sécurité et de la continuité de la TI [DSCTI]
- DGIST : Direction générale de l'information, des sciences et de la technologie – y compris la liaison avec SPC et l'Agence du revenu du Canada (ARC)
- GI : Gestion de l'information

| | **CGEPPS** | **ASM** | **CSTI** | **DGIST** | **GI** |
|---|---|---|---|---|---|
| ***Pistes de vérification du système d'information*** | | | | | |
| Définir et examiner les évènements vérifiables | A+R | R | C | | |
| Définir le contenu des dossiers de vérification | A+R | R | C | | |
| Définir les actions permises | A+R | C | C | | |
| Valider les capacités de production des | A+R | R | C | | |

| | CGEPPS | ASM | CSTI | DGIST | GI |
|---|---|---|---|---|---|
| dossiers de vérification | | | | | |
| Maintenir la capacité de stockage des dossiers de vérification | A+R | C | C | R | |
| Définir les interventions en cas d'échec de vérification | A+R | R | C | C | |
| Inscrire l'heure système sur les pistes de vérification | A+R | C | C | R | |
| Protéger les dossiers de vérification dans le système d'information | A+R | C | C | C | |
| Sauvegarder les dossiers de vérification | A+R | C | C | R | |
| Définir la conservation et l'élimination | A+R | R | C | | R |
| ***Capacité globale de l'ASFC*[2]** | | | | | |
| Protéger les dossiers de vérification dans le SCGPV | | A+R | | R | |
| Centraliser les pistes de vérification dans le SCGPV | R | A+R | C | C | |
| Fournir une capacité de réduction des vérifications et d'établissement | C | A+R | | C | |

[2] L'ASM est le responsable opérationnel chargé du Système central de gestion des pistes de vérification; il assure la collecte, la gestion et l'examen adéquats et sécuritaires des journaux de vérification. La DGIST est le responsable technique chargé des opérations techniques.

| | CGEPPS | ASM | CSTI | DGIST | GI |
|---|---|---|---|---|---|
| de rapports dans le SCGPV | | | | | |
| Fournir la synchronisation temporelle | | C | | A+R | |
| Examiner les journaux de vérification et intervenir | C | A+R | C | C | |
| Gérer le réglage de la quantité d'examens | R | A+R | C | R | |
| Fournir des rapports de connaissance de la situation | C | A+R | C | C | |

# 7. Conformité et établissement de rapports

L'ASM, le Coordinateur de la Sécurité des TI, les praticiens de la sécurité et les gestionnaires sont responsables pour la surveillance de la conformité avec cette norme dans l'ASFC, et pour mesurer l'efficacité de la gestion des dossiers de vérification.

Les employés doivent rapporter les incidents de sécurité conformément aux procédures détaillées dans le Volume de Sécurité de l'ASFC, Rapport des incidents de sécurité.

# 8. Conséquences

L'ASM est responsable de mener des enquêtes et d'intervenir lorsque des cas de non-conformité de la présente norme sont signalés. De plus, il doit veiller à ce que les mesures correctives appropriées soient prises, au besoin. S'il est déterminé qu'un employé a enfreint les politiques, les directives ou les normes, celui-ci pourrait faire l'objet d'un examen justifié des enquêtes de sécurité ainsi que de mesures disciplinaires pouvant aller jusqu'au licenciement.

# 9. Examen de la norme

Cette norme sera revue tous les trois ans ou plus fréquemment comme déterminé par l'ASM et le CSTI.

# 10. Définitions

| Termes | Définition |
|---|---|
| Dossier de vérification | Le dossier officiel d'un événement de TI. |
| Gestion des pistes de vérification | Le processus de production, de transmission, de stockage, d'analyse et d'élimination des dossiers de vérification. |
| Événement | Pour ce qui est des systèmes de technologie de l'information (TI), un incident qui se produit dans un système d'information (au niveau de l'infrastructure ou de l'application). |

# 11. Références

## 11.1. ASFC

- Directive sur la gestion du risque en matière de sécurité des TI

## 11.2. Secrétariat du Conseil du Trésor

- Politique sur la sécurité du gouvernement
- Cadre stratégique pour l'information et la technologie
- Politique sur l'accès à l'information
- Politique sur la vérification interne
- Politique sur la gestion des technologies de l'information
- Politique sur la protection de la vie privée
- Directive sur la tenue de documents
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)

## 11.3. Centre de la sécurité des télécommunications Canada

- ITSG-33 du CSTC : Gestion des risques relatifs à la sécurité de la TI

## 11.4. Demandes de renseignements

Pour obtenir des conseils au sujet de la présente norme, communiquer avec :

Division de la sécurité et de la continuité des opérations de la TI
Direction des services organisationnels
Direction générale de l'information, des sciences et de la technologie
CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca

Ou

Division de l'infrastructure et de la sécurité de l'information
Direction de la sécurité et des normes professionnelles
Direction générale du contrôle
Information_Security-Securite_de_linformation@cbsa-asfc.gc.ca

Canada Border Services Agency | Agence des services frontaliers du Canada



# Policy on the Use of Electronic Resources

PROTECTION • SERVICE • INTEGRITY

Canada



# 1. Effective Date

This policy is effective immediately upon issuance. This version of the policy replaces version 1.1 (04 Jan 2011). It incorporates updates to departmental references and definitions effective May 13, 2013.

# 2. Policy

The Canada Border Services Agency (CBSA) policy on the use of electronic resources is based on the Treasury Board of Canada Secretariat Policy on Acceptable Network and Device Use.

# 3. Policy Objective

The objective of this policy is to ensure that individuals who access the Agency's systems and electronic resources, including electronic networks and systems shared with the Canada Revenue Agency (CRA), Shared Services Canada (SSC) and Citizenship and Immigration Canada (CIC), use the electronic resources appropriately.

This policy also sets out the obligations and responsibilities of users with respect to the appropriate use of CBSA's electronic resources.

# 4. Application

This policy applies to all individuals who access CBSA's electronic resources.

# 5. Context

CBSA uses many electronic resources: computer networks, servers, workstations, standalone computers, peripherals, storage devices, handheld devices and other devices for creating, collecting, storing, transmitting, and processing information that are critical to its daily operations. Adopting and applying a common set of policies is essential to ensure effective, efficient and secure operations.

CBSA is subject to the Treasury Board Secretariat (TBS) Policy on Government Security and to the TBS Policy on Acceptable Network and Device Use.

These policies set out:

- access to Government of Canada electronic networks, whether from inside or outside of government buildings
- the acceptable and unacceptable use of these networks
- user and management responsibilities







- corrective and disciplinary measures
- processes for monitoring networks

The Treasury Board Secretariat requires that government departments have policies and procedures for the appropriate use of electronic networks and resources. Departments must also ensure the confidentiality, integrity and availability of their information technology (IT) assets and information by applying proper safeguards against evolving threats.

# 6. Definitions

**Access**

Gaining entry to or using an electronic resource that CBSA has provided to authorized individuals. Access to such resources may be from inside or outside government premises. Access includes telework and remote access situations or where authorized individuals are using electronic resources provided by CBSA on their own time for limited personal use as defined in this policy.

**Audit**

The collection and recording of user activities, including file access.

**Authorized individuals**

CBSA employees, contractors/consultants and other persons who have been authorized by management to access CBSA's electronic resources.

**Electronic resources**

Computers, computer networks and systems, functions, and devices for users or programs. These resources include the Internet, CBSA software and devices, and public or private devices. Also included is hardware such as standalone computers, laptops, peripherals, memory devices, wireless devices, and any other media used to obtain, store, or send information (e.g. USB keys, tablets, smart phones, etc.). Many non-computing devices, such as digital cameras and cellular phones, are considered electronic resources under this policy because they can store and send information. Infrastructure and network services the SSC and the CRA provides to CBSA and network services between CBSA and other government organizations are also considered electronic resources.

**Monitor**

The continuous checking of network and system activity for abnormal, unlawful, inappropriate, criminal or unusual activity.

**Monitoring of electronic resources**

The recording and analysis of the use of electronic resources for operational purposes and for assessing compliance with government policy.

For additional definitions of terms, refer to Annex E of this document or the ISTB Glossary. (Enter IT Security to return IT Security terms only)



# 7. Policy Statement

CBSA employees use electronic resources to conduct the business of government. This includes communicating with other government employees and the public, gathering information relevant to their duties, on a need to know basis, and developing expertise in using such resources.

CBSA's electronic resources are for business purposes. Limited personal use, as defined in this policy, of e-mail, Microsoft Office programs, or the Internet is allowed on the condition that users comply with all applicable CBSA, federal and provincial policies and legislation. All information obtained, stored or disseminated using CBSA's electronic resources and any activity performed by individuals on these systems may be monitored. In its monitoring practices, the Agency will respect the users' and the clients' rights to privacy and will ensure a reasonable balance between users' expectations of privacy and the organization's duty to protect information and assets. Security incidents will be reported and investigations will be carried out when necessary. Electronic records are subject to Access to Information and Privacy (ATIP) requirements and requests. Any individual breaching this policy will be subject to disciplinary action up to and including termination of employment.

# 8. Policy Requirements

All federal laws and applicable federal government policies on the use of electronic resources apply to CBSA's computer systems and electronic resources.

This Policy should be read in concurrence with the Directive on the Appropriate Use of E-mail and the Directive on the Use of Wireless Technology.

Electronic records may be accessible under the Access to Information Act and the Privacy Act, subject to exemptions under those Acts.

# 9. Acceptable Use of Electronic Resources

Electronic resources shall be used for official business to carry out the mandate and mission of CBSA. Authorized individuals must use only Agency-authorized applications, hardware and software installed by CBSA/CRA authorized IT staff.

CBSA's electronic resources are to be used for approved purposes, namely:

a. Conducting government business, such as:
    - Communicating and sharing information with colleagues, other government departments and the private sector in the performance of CBSA functions and activities;
    - Conducting research for Agency purposes;
    - Gathering information relevant to a user's duties;
    - Developing expertise in using electronic resources effectively and efficiently; and
    - Undertaking professional development activities that are job related.







b. Limited personal use (during lunch break, periods of rest or before or after work as specified in the CBSA Code of Conduct), such as:
   - Communicating with family, friends and other persons for non-official purposes;
   - Accessing acceptable news and other information sources that are not prohibited or restricted by law or policy;
   - Conducting routine personal banking transactions; and
   - Any union activity or business specifically pre-authorized in writing by your manager.

c. Any other purpose that is consistent with the Treasury Board of Canada Secretariat Policy on Acceptable Network and Device Use and this policy or is specifically authorized in writing by management.

## Conditions of limited personal use

Limited personal use of e-mail, Microsoft Office programs, or the Internet is permitted on the condition that users comply with all applicable CBSA, federal and provincial policies and legislation. All other electronic resources and systems are for Agency business purposes only, and their use is limited to activities directly related to an authorized user's official duties.

Limited personal use must not:

a. Interfere with a user's productivity or performance of official duties and functions,
b. Incur any direct costs to the Agency,
c. Involve a criminal, unlawful or unacceptable activity as defined in this policy, and
d. Impose a performance or storage burden on the Agency's electronic resources.

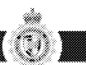
CBSA may restrict or prohibit any authorized use of CBSA electronic resources and networks if:

a. The use threatens the capability or integrity of CBSA electronic networks, resources and computers; or
b. The restriction or prohibition is otherwise necessary for operational or administrative issues.

## E-mail

E-mail is a business communication tool that is critical to the Agency's daily operations and business. The use of the Agency's e-mail for unacceptable or unlawful activities, such as a personal business or to assist relatives, friends or other persons in such activities, is expressly prohibited. Use of e-mail for union notices or other union material requires prior written approval of the Agency.

E-mail is subject to all legislation governing written communications, including the Access to Information Act, the Privacy Act, the Library and Archives of Canada Act, the Official Languages



Act, the Canadian Human Rights Act, and the Criminal Code. Under the Access to Information Act and the Privacy Act, the public may have access to electronic records, subject to applicable exemptions under those Acts.

For more details on e-mail, refer to the CBSA Directive on the Appropriate Use of E-mail .

## Corporate and transitory information

All information, including e-mail, (in any physical or electronic form) created, stored, received or transmitted via electronic resources that contains information on CBSA functions, actions and decisions must be retained and preserved. All users are responsible for the effective management of all information they create and store. Information must be preserved and protected from unauthorized destruction and access. Further details on corporate and transitory information can be obtained from the CBSA Information Management (IM) Policy and the Treasury Board Secretariat Policy on Information Management.

# 10. Unacceptable Use of Electronic Resources

CBSA electronic resources shall not be used to operate unauthorized software or applications such as games or other entertainment software under any circumstances unless specifically authorized by CBSA[1]. Individuals must not access CBSA information about themselves, their colleagues, their relatives, their acquaintances or other non-work-related individuals under any circumstances, except where access to that information is directly related to an authorized program or activity that the individual is specifically authorized to perform. Access to CBSA systems and information is on a "need-to-know" basis. This means that access to specific information and to specific information systems is limited to authorized individuals with the appropriate security screening level and specific official job-related requirements. The information that a user accesses is considered privileged and is not to be shared, discussed or disclosed to others. Users' access must be reviewed when their duties or status change.

# 11. Criminal, Unlawful, and Unacceptable Activities

There are three categories of inappropriate activities that relate to electronic resources: criminal activities; unlawful, but non-criminal activities; and unacceptable activities.

CBSA's electronic resources shall not be used to conduct:

1. Any criminal activity (e.g., child pornography, obscenity, copyright violation, defamation, hacking, harassment, hate propaganda);
2. Any unlawful, but not criminal, activity that includes regulatory offences or other contraventions of federal and provincial statutes and regulations, and actions that make an authorized individual or the agency liable to a civil lawsuit (e.g., destroying data, disclosing sensitive information, posting inaccurate information); and



3. Any activity that, although legal, is unacceptable and that violates Agency or Treasury Board policy (e.g., sending classified information on unsecured networks, sending abusive, sexist or racist messages, representing personal opinions as those of CBSA).

If there are reasonable grounds to suspect criminal, unlawful or unacceptable use of the electronic resources, these activities are to be reported to your manager.[2]

A non-comprehensive list of these types of activities is included in Annexes A, B and C. Additional examples of misuse are included in Annex D.

---

[1]Personally-owned electronic devices, (e.g. home computer, smart phones, tablets, etc.) are not to be used to process CBSA information. Employees should not connect their personal electronic devices to computer equipment from the CBSA, for example, power charging a personal device from a USB port.

[2]Authorized employees may need to access restricted sites, such as those with pornography or hate propaganda, while conducting authorized investigations or intelligence activities or when researching or developing CBSA-sanctioned documents such as training materials. CBSA employees may be required to view all types of material to determine their admissibility.

# 12. Roles and Responsibilities

## Authorized individuals

Everyone who uses CBSA's electronic resources must comply with this policy, all applicable government policies and laws. Users will be held accountable for all activities they perform using CBSA's electronic resources.

Authorized users are responsible for becoming familiar with this policy and adhering to it every time they access or use the Agency's electronic networks and resources.

Authorized individuals are responsible for using CBSA's electronic resources in an appropriate manner, such as by:

a. Protecting their passwords, user identification or computer accounts to prevent use by others;
b. Reporting instances of misuse and unacceptable or unlawful activities, such as chain letters and viruses;
c. Being aware of information technology security policies and any issues published by the Chief Information Officer (CIO) or the Departmental Security Officer (DSO);
d. Using information technology security features (encryption, virus protection) provided by CBSA, as required;
e. Communicating in a manner that reflects positively on the mandate and mission of CBSA; and



f. Obtaining clarification from the Director of Information Technology Security and Continuity or the Departmental Security Officer when in doubt whether a planned use is acceptable and lawful according to this policy.

## Managers

Managers are responsible for:

a. Determining and approving their staff's specific system access;
b. Informing their staff of their responsibilities on the appropriate use of CBSA's electronic resources;
c. Reporting instances of suspected or alleged criminal, unlawful or unacceptable uses of CBSA's electronic resources to the Security and Professional Standards Directorate;
d. Addressing quickly, fairly and decisively any violations of policy or law; and
e. Ensuring that no corporate information remains on the user's network drive when the person leaves CBSA (i.e., retirement, secondment, assignment).

## Director General, Infrastructure Services Directorate

The Director General, Infrastructure Services is responsible for:

a. Providing training or information on using electronic resources effectively and efficiently;
b. Establishing procedures for granting access to CBSA's electronic resources; and
c. Establishing procedures, in collaboration with the Director General of the Security and Professional Standards Directorate (SPSD) or the DSO, for granting access to the Internet via CBSA's electronic resources

## Departmental Security Officer (DSO)

The Departmental Security Officer is responsible for:

a. Providing clarification on this policy;
b. Providing information on the interpretation of lawful and acceptable use of CBSA's electronic resources;
c. Approving the individuals who are authorized to monitor the use of electronic resources;
d. Referring managers to the Security and Professional Standards Directorate for requests involving accessing electronic e-mail messages or files located in a user's account;



e. Referring managers to the Security and Professional Standards Directorate when there is suspected misuse of the Agency's electronic resources;
f. Investigating reports of suspected criminal, unlawful or unacceptable uses of CBSA's electronic resources;
g. Seeking advice from Labour Relations and Legal in cases of suspected criminal or unlawful uses of CBSA's electronic resources and reporting to law enforcement authorities, when necessary; and
h. Responding to any requests pertaining to the Access to Information Act that are relevant to this policy.

## IT operational personnel

Under the general direction of the IT Security Coordinator, IT operational personnel are responsible for:

a. Understanding and complying with CBSA IT security policies and procedures to protect IT operations and infrastructure;
b. Responding to and reporting security incidents to their immediate manager and then to the Security and Professional Standards Directorate;[2]
c. Testing and installing security patches according to agency procedures; and
d. Maintaining and upgrading hardware and software and controlling the infrastructure's configuration by using effective change control and configuration management practices.

---

[2] When there is suspected misuse of Agency electronic resources, IT operational personnel are not authorized, without approval, to take any immediate action since it may adversely affect any possible future investigation.

# 13. Privacy and Monitoring

## Expectations of privacy

The Government Security Policy recognizes that:

a. The Canadian Charter of Rights and Freedoms guarantees that government authorized individuals have a right to a reasonable expectation of privacy, and this right extends to the workplace.
b. Authorized individuals also have protection under the Privacy Act, with limits placed on the organization's authority to search employees and their effects.



CBSA is also subject to reasonable privacy expectations of its clients under the Privacy Act and the Customs Act (sections 107 and 160).

## Monitoring of electronic resources

Monitoring is done to make sure users comply with this policy. The Agency's monitoring practices respect the privacy of its users and clients. There is a reasonable balance between an individual's privacy and the organization's duty to protect sensitive information and assets (including all electronic resources) and to conduct its activities efficiently and lawfully.

CBSA conducts three types of monitoring:

### 1. Monitoring for operational purposes

The Infrastructure Services Directorate is responsible for monitoring electronic resources for operational reasons. Its must determine whether the resources are operating efficiently in order to isolate and resolve problems and to assess compliance with government policy. In addition, periodic and random checks of the resources for specific operational purposes can occur, and the resulting information can be analyzed.

Normal routine analysis does not involve reading the content of electronic mail, files or transmissions. It may involve:

a. Identifying the size and type(s) of file(s) suspected of causing problems;
b. Identifying patterns of use;
c. Determining the sender, the intended recipient and the subject line of e-mail messages;
d. Keyword searches of files on electronic resources including network servers or on computer storage devices; and
e. Searching for malicious codes and illegal, unlawful, unusual and unacceptable activities or behaviour.

### 2. Content monitoring

The Security and Professional Standards Directorate is responsible for monitoring the content of individual's e-mail records and other files. CBSA's electronic network automatically logs the identity of individuals and their activities while on the network.

Copies of files and e-mail records (including "deleted" records) may be accessible under the Access to Information Act and the Privacy Act, subject to exemptions under those Acts.

### 3. Monitoring for unlawful activity/unacceptable conduct

If there are reasonable grounds to suspect that an individual is misusing the Agency's electronic resources-due to a routine analysis or a complaint-the matter shall be referred to Security and Professional Standard for further investigation. They can authorize monitoring without notice,







including reading or viewing the content of individual e-mail records or other files. If misuse of the electronic resources has occurred, refer to the "Disciplinary Measures" section of this policy.

## 14. Investigations

In the event that authorized individuals conduct an investigation and are required to read the contents of electronic communications and records, they are bound by law to protect sensitive, confidential information and use it only for authorized purposes. Investigations must be conducted in accordance with the Canadian Charter of Rights and Freedoms, the Privacy Act, the Criminal Code and CBSA procedures on internal investigations.

## 15. Disciplinary Measures

CBSA will report suspected unlawful and criminal use of its electronic resources to law enforcement authorities after consultation with Labour Relations and its legal advisors.

CBSA may take disciplinary measures in cases of unlawful, criminal or unacceptable use of its electronic resources. Disciplinary measures will be commensurate with the seriousness and circumstances of the incident.

Disciplinary measures may include:

a. An oral or written reprimand;
b. Limitations on access to the electronic resources; and/or
c. Suspension or termination of employment.

Disciplinary measures will be taken against contractors or other individuals authorized to use CBSA's electronic resources as specified in the conditions-of-use agreement included as an appendix or attachment to the contract.

For more details regarding disciplinary measures, refer to the CBSA Code of Conduct, the CBSA Discipline Policy and the Discipline Guidelines and all other applicable policies and guidelines.

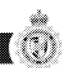
## 16. Policy Review

This policy shall be reviewed at least every five years by the Director General, Infrastructure Services and the Director General, Security and Professional Standards and Departmental Security Officer (DSO).

## 17. References

### Related Legislation and Policies

CBSA Code of Conduct
CBSA Discipline Policy and Discipline Guidelines



Values and Ethics Code for the Public Sector
Financial Administration Act
Access to Information Act
Privacy Act
Charter of Rights and Freedoms
Customs Act, Section 107
Explanation of section 107 of the customs act
Library and Archives of Canada Act
Security of Information Act
Criminal Code
Export and Import Permits Act
Crown Liability and Proceedings Act
Copyright Act
Trade-marks Act
Patent Act
Canadian Human Rights Act
Official Languages Act

## Cross-references

### Treasury Board Policies and Publications

Guidelines for Discipline
Prevention and Resolution of Harassment in the Workplace
Policy on Government Security
Government Communications Policy
Policy on Information Management
Management of Information Technology Security (MITS)
Access to Information Policy
Access to information and privacy
Policy on Acceptable Network and Device Use
Telework Policy
Directives on Losses of Money or Property

# 18. Enquiries

Enquiries regarding this policy should be addressed to:
**Information, Science & Technology Branch**
IT Security and Continuity
Email: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca
Intranet: IT Security

**Comptrollership Branch**
Security & Professional Standards Directorate
Email: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca



# Annex A

## Criminal Offences

**(Non-Exhaustive List of Examples)**

The following are examples of criminal activity that could take place on electronic networks and resources.

a. **Child pornography:** Possessing, downloading or distributing any child pornography (see s. 163.1 of the Criminal Code).
b. **Copyright:** Infringing on another person's copyright without lawful excuse. The Copyright Act provides for criminal prosecutions and civil actions in such cases (see also "copyright" under violations of federal and provincial statutes).
c. **Defamation:** Causing a statement to be read by others that is likely to injure the reputation of any person by exposing that person to hatred, contempt, or ridicule or that is designed to insult the person (see ss. 296-317 of the Criminal Code).
d. **Hacking and other crimes related to computer security - Gaining unauthorized access to a computer system:** Using someone else's password or encryption keys to engage in fraud or obtaining money, goods or services, or accessing information through false representations made on a computer system. See the following Criminal Code provisions: s. 122 (breach of trust by public officer); s. 380 (fraud); s. 361 (false pretences); s. 403 (fraudulent personation); s. 342.1 (unauthorized use of computer systems and obtaining computer services).
e. **Trying to defeat the security features of the electronic networks:** See the following Criminal Code provisions: s. 342.1 (unauthorized use of computer systems and obtaining computer services); s. 342.1(d) (using, possessing or trafficking in stolen computer passwords or stolen credit card information); s. 342.2 (making, possessing or distributing computer programs that are designed to assist in obtaining unlawful access to computer systems); ss. 429 and 430 (mischief in relation to data).
f. **Spreading viruses with intent to cause harm:** See the following Criminal Code provisions: ss. 429 and 430 (mischief in relation to data); s. 342.1 (unauthorized use of computer systems and obtaining computer services).
g. **Destroying, altering or encrypting data without authorization and with the intent of making it inaccessible to others with a lawful need to access it:** See the following Criminal Code provisions: ss. 429 and 430 (mischief in relation to data); s. 342.1 (unauthorized use of computer systems and obtaining computer services); ss. 129 and 139(2) (destroying or falsifying evidence to obstruct a criminal investigation).
h. **Interfering with others' lawful use of data and computers:** See the following Criminal Code provisions: ss. 429 and 430 (mischief in relation to data); s. 326 (theft of telecommunication services); s. 322 (theft of computer equipment); s. 342.1 (unauthorized use of computer systems and obtaining computer services).
i. **Harassment:** Sending electronic messages, without lawful authority, that cause people to fear for their safety or the safety of anyone known to them (see s. 264 of the Criminal Code). Section 264.1 of the Criminal Code makes it an offence to send threats to cause serious bodily harm, damage personal property or injure a person's animal.
j. **Hate propaganda:** Disseminating messages that promote hatred or incite violence against identifiable groups in statements outside of private conversations (see s. 319 of the Criminal Code).



k. **Interception of private communications or electronic mail (in transit):** Unlawfully intercepting someone's private communications or unlawfully intercepting someone's electronic mail (see s. 184 and s. 342.1 of the Criminal Code, respectively).
l. **Obscenity:** Distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material (e.g., material showing explicit sex where there is undue exploitation of sex, where violence or children are present, or where the sex is degrading or dehumanizing and there is a substantial risk that the material could lead others to engage in anti-social acts). See s. 163 of the Criminal Code.
m. **Various other offences:** The Criminal Code (and a few other statutes) provide for a range of other offences that can take place in whole or in part using electronic networks. For example, fraud, extortion, blackmail, bribery, illegal gambling, and dealing in illegal drugs can all occur, at least in part, over electronic networks and are criminal acts.



# Annex B

## Unlawful Activity that Violates Federal and Provincial Statutes

**(Non-Exhaustive List of Examples)**

The following are examples of unlawful (though not criminal) activity that can take place on electronic networks and resources.

a. **Copyright and intellectual property:** Violating another person's copyright (the Copyright Act provides for criminal prosecutions and civil actions in such cases). Unauthorized use of trade-marks and patents can also occur on electronic networks and these acts are proscribed in the Trade-marks Act.
b. **Defamation:** Spreading false allegations or rumours that would harm a person's reputation. In addition to criminal libel, defamation is contrary to provincial statutes dealing with this subject.
c. **Destroying or altering data without authorization:** Unlawfully destroying, altering or falsifying electronic records. See the following provisions: s. 5 of the National Archives of Canada Act; ss. 6 and 12 of the Privacy Act; s. 4 of the Access to Information Act; s. 5 of the Official Secrets Act.
d. **Disclosing sensitive information without authorization** - **Disclosing personal information:** Failing to respect the privacy and dignity of every person. The obligation to respect a person's privacy is expressed in a number of statutory provisions, such as ss. 4, 5, 7 and 8 of the Privacy Act and s. 19(1) of the Access to Information Act. Many federal statutes have non-disclosure provisions, often designed to protect the privacy of citizens who provide information to the government (see list of provisions in Schedule II of the Access to Information Act). In addition, Quebec has a number of privacy provisions in its Civil Code (see articles 3, 35-41) and in its Human Rights Charter (see articles 4, 5 and 49). British Columbia, Saskatchewan, Manitoba and Newfoundland also have statutes that provide for civil actions where there is an undue invasion of privacy.
e. **Disclosing business trade secrets:** Revealing business trade secrets without authorization or in response to a formal request under the Access to Information Act, business trade secrets or confidential commercial information supplied in confidence by a third party and consistently treated as confidential by the third party. See s. 20(1)(a) and (b) of the Access to Information Act.
f. **Disclosing sensitive government information:** Revealing sensitive government information without authorization. See ss. 3 and 4 of the Official Secrets Act. As well, when responding to formal requests under the Access to Information Act, institutions

must not disclose information obtained in confidence from other governments (see s. 13 of the Access to Information Act. The other exemptions in the Act relating to government information are discretionary.

Note that employees and other authorized individuals and the government are immune from legal actions with respect to disclosures made in good faith under either the Privacy Act or Access to Information Act.

g. **Harassment:** It is a discriminatory practice "(a) in the provision of [...] services [...] available to the general public [...] or (c) in matters related to employment to harass an individual on a prohibited ground of discrimination". The prohibited grounds are race, national or ethnic origin, colour, religion, age, sexual orientation, marital status, family status, disability and conviction for which a pardon has been granted. Thus, in some circumstances, displaying unwelcome sexist, pornographic, racist or homophobic images or text on a screen at work can be unlawful harassment. See s. 14 of the Canadian Human Rights Act.
h. **Privacy infractions:** Reading someone else's electronic mail or other personal information without authorization, listening in on someone's private conversations or intercepting electronic mail while it is in transit, for example.

   When an employee or other person has a reasonable expectation of privacy in his or her electronic mail or other personal documents, an institution may be guilty of an unreasonable search or seizure under s. 8 of the Charter of Rights and Freedoms if it infringes on that reasonable expectation without a lawful authority. This is true whether the institution is acting as employer or otherwise.

   The institution may also be deemed to have collected or used data unlawfully, contrary to ss. 4, 5, 7 and 8 of the Privacy Act. The government may be liable for damages when private communications are intercepted unlawfully. See ss. 16-20 of the Crown Liability and Proceedings Act concerning electronic surveillance activities carried out by Crown servants in the course of their employment; s. 20 specifically provides that the Crown servant will be accountable to the Crown for the amount of the damages awarded by a court. The government may also be liable for damages when an unlawful disclosure of personal information occurs contrary to provisions in various statutes (see the list of such provisions in Schedule II of the Access to Information Act). For more information on these issues, refer to Appendix E of the Treasury Board Policy on the Use of Electronic Networks, which discusses reasonable expectations of privacy.
i. **Use of public money without proper authority:** See the following provisions of the Financial Administration Act: s. 33 (making a requisition without authority); s. 34 (certifying receipt



of goods or services without authority); s. 78 (liability for losses caused by malfeasance or negligence); and s. 80 (taking bribes or participating in corrupt practices).

## Activity that can expose authorized individuals or the employer to civil liability

Various kinds of conduct can expose a person or an employer to civil liability. The employer's liability will be triggered when a Public Service employee performs the unlawful activity in the course of his or her employment. The Public Service employee remains liable for these actions, even when the federal government is also liable. (The government's policy on indemnifying authorized individuals - Policy on the Indemnification of and Legal Assistance for Crown Servants - is relevant to such actions.) The following are examples of civil wrongs that can take place on electronic networks.

a. **Disclosing or collection of sensitive data:** revealing or obtaining such information without authorization. In addition to the statutory provisions mentioned above, an unauthorized disclosure or collection of personal information can result, in some circumstances, in a civil action for invasion of privacy, nuisance or trespass under common law, and similar actions under the Civil Code of Quebec (articles 3, 15-41); for breach of contract and for breach of trust or breach of confidence (e.g. if confidential commercial information is disclosed).
b. **Defamation:** spreading false allegations or rumours that would harm a person's reputation. In addition to criminal libel, publishing defamatory statements without a lawful defence can result in a civil action.
c. **Inaccurate information:** posting inaccurate information, whether negligently or intentionally. This can lead to civil lawsuits for negligent misrepresentation if it can be shown that (a) the posting caused harm and resulted in damages to the person who (b) reasonably relied on the information, that (c) the person or institution that made the posting owed a duty of care to the person who was harmed by inaccurate information; and (d) the inaccuracy was due to negligence (conduct that falls below what is reasonable in the circumstances).



# Annex C

## Unacceptable Activity that Is Not Necessarily Unlawful but that Violates Treasury Board and/or CBSA Policies

**(Non-Exhaustive List of Examples)**

A number of Treasury Board policies are not media-specific - that is, they apply whether the unacceptable activity occurs on paper, by telephone, through computer networks, in oral conversation or through any other medium. It is unacceptable to violate Treasury Board and/or CBSA policies including institutional policies. The following policies are important in the context of the use of electronic resources: the Policy on Government Security (in relation to standards including the Operational Security Standard: Management of Information Technology Security (MITS); the Prevention and Resolution of Harassment in the Workplace Policy; the Privacy and Data Protection Policy, including the Employee Privacy Code; the Government Communications Policy; the Value and Ethics Code for the Public Service and the CBSA Code of Conduct These policies relate to various activities, as described below.

a. **Sending classified or protected information on unsecured networks:** Unless it is sent in encrypted form. (Government Security Policy and this CBSA policy)
b. **Accessing, without authorization, sensitive information held by the government:** (Government Security Policy)
c. **Attempting to defeat information technology security features:** Through such means as using anti-security programs; using someone else's password, user identification or computer account; disclosing one's password, network configuration information or access codes to others; or disabling anti-virus programs. (Government Security Policy)
d. **Causing congestion and disruption of networks and systems** Through such means as sending chain letters and receiving list server electronic mail unrelated to work. These are examples of excessive use of resources for non-work-related purposes. (Government Security Policy)
e. **Sending abusive, sexist or racist messages to employees and other individuals:** (Prevention and Resolution of Harassment in the Workplace Policy)
f. **Using the government's electronic networks for private business, personal gain or profit or political activity:** (TBS Policy on Electronic Networks)
g. **Making excessive public criticisms of governmental policy:** (CBSA Code of Conduct and Value and Ethics Code for the Public Service)
h. **Representing personal opinions as those of the institution or otherwise failing to comply with institutional procedures concerning public statements about the government's positions:** (CBSA Code of Conduct and Value and Ethics Code for the Public Service)
i. **Failing to provide employees and other authorized individuals with notice of electronic monitoring and auditing practices:** (Government Security Policy and the Employee Privacy Code)
j. **Providing personnel with access to systems, networks, or applications used to process sensitive information before such personnel are properly security screened:** (Government Security Policy)



k. **Failing to revoke system access rights of personnel, when they leave the institution, at the end of employment or the termination of a contract, or when they lose their reliability status or security clearance:** (Government Security Policy)

l. **Unauthorized removal or installation of hardware or software on government-owned informatics devices or electronic networks:** (Government Security Policy)



# Annex D

## Additional Examples of Inappropriate/Misuse of CBSA's Electronic Resources

The following actions are examples of breaches of this policy and are subject to disciplinary action.

Unacceptable use of the Agency's electronic resources include, but are not limited to, obtaining, storing, sending, or participating in:

- Chain letters, pyramid schemes, offensive material or material containing pornography, nudity, profane language, violence or sexual content;
- Unauthorized gambling pools;
- Disclosing or sharing your password, user account or other credentials;
- Material related to the promotion or use of illegal substances;
- Attempting to defeat information technology features, through such means as using anti security programs, using another user's password, User ID or network accounts, disclosing a password or removing or modifying installed security features;
- Using the Agency's electronic networks to conduct private business, for personal gain or profit, or for political activity;
- Sending hate propaganda (may also be criminal)
- Participating in an unauthorized gambling activity for personal gain;
- Subscribing to mailing lists, newsgroups and chat rooms not related to the performance of your duties;
- Installing, storing, using, modifying or sending games, unauthorized software, script files or batch files;
- Installing or retiring software or hardware, or modifying its functionality, unless you are an IT operational staff member authorized to maintain them;
- Installing screen savers without the authorization of IT operational personnel, and
- Not taking precautionary measures for virus prevention



# Annex E

## Terms and Definitions

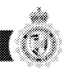
Here is an alphabetical list of terms found in this policy: the CBSA Policy on the Use of Electronic Resources. This is a reference guide to help users understand the policy.

**Assets** are tangible or intangible things of the Government of Canada. Assets include, but are not limited to, information in all forms and media, networks, systems, material, real property, financial resources, employee trust, public confidence and international reputation.
**Availability** is the condition of being usable on demand to support operations, programs and services.
**Chain letters** are e-mail messages with a single intent: to have you forward them to others. They falsely offer luck, money or a wish if you send them on.
**Chat rooms** are electronic forums where participants can have on-line discussion in real time, normally through the exchange of text messages.
**Classified information** is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest. (See also Sensitive Information)
**Compromise** includes injury due to unauthorized disclosure, destruction, removal, modification, interruption or use of assets.
**Confidentiality** is the attribute that information must not be disclosed to unauthorized individuals because of the resulting injury to national or other interests, with reference to specific provisions of the Access to Information Act and the Privacy Act.
**Content administration** may include, but is not limited to, installing out-of-office messages or extracting corporate documents.
**Content monitoring** may include, but is not limited to, viewing the content and analyzing the volume of files, e-mail messages or logs to determine whether misuse has occurred.
**Corporate information** is recorded information derived from the actions, transactions, business processes, functions and activities of the CBSA. It serves as:

- evidence on organizational performance;
- an account of resource use;
- an account of how and why decisions were made;
- the method to certify compliance with legislation, policies and standards;
- the method to demonstrate how transactions are tracked over time;
- a memory about the work environment and governing factors;

- a testimony of the rights and entitlements of employees, individuals, corporations, etc.; and
- a record that documents the activities that support and protect the legal, financial, historical and other interests of the government and the public.

**Gambling** is to bet, wager or risk money or something of value on a game of chance or mixed skill and chance. It may take many forms and includes sports pools and other types of pools.
**Information** is a corporate asset or resource, which is defined as data, facts or knowledge that is recorded, regardless of form, recording media, or technology used.
**Information technology security** involves safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.
**Integrity** is the accuracy and completeness of assets and the authenticity of transactions.
**Misuse** means any action or inaction by a user that constitutes an unacceptable activity, an unlawful activity or a criminal activity.
**Nudity** is a naked person or a person displaying genitalia. Does not need to be sexual in content.
**Offensive material** is likely to insult, disgust or repulse. These include jokes made against select groups (e.g., racial, religious, or sexist jokes). It may also include offensive images (e.g., images of corpses, portrayals of defecation).
**Phishing** is a form of Internet fraud that uses authentic-looking but false e-mails, Web sites or other information to steal valuable information such as credit cards, social insurance numbers, user IDs and passwords.
**Pornography** is explicitly sexual material designed or intended to cause sexual arousal or titillation.
**Primary systems** are databases such as CAS, mainframe applications and network applications. They are provided for Agency business purposes only.
**Private business** is an activity outside the scope of employment conducted for personal gain or profit. This includes the sale or purchase of any goods or services. This category also includes the conduct of political activity.
**Profanity** includes material where offensive language is used. It includes, but is not limited to, vulgar language in a written text, oral use of the words in a sound file or video, or even a caption with an image.
**Protected information** is information not related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or the Privacy Act, and the compromise of which would reasonably be expected to cause injury to a non-national interest. (See also Sensitive Information.)



**Pyramid schemes** are hierarchies in which you are encouraged to send money with the expectation that a set number of individuals will in turn send you money.
**Records** are information in any physical or electronic form, including audio-visual records, photographs, maps, drawings, film, sound recording, videotape, microform, magnetic tape, paper or electronic files, and any other documentary material.
**Risk** is the chance of a vulnerability being exploited or resulting in harm.
**Secondary systems** are comprised of applications such as e-mail, Microsoft Office and Internet (where limited personal use is permitted).
**Security incident** is the compromise of an asset, or any act or omission that could result in a compromise, threat or act of violence toward employees.
**Sensitive information** is information that must be afforded appropriate safeguards because of its confidential nature. (See also Classified information and Protected information.)
**Sexual content** is material where the sexual act may not be explicit (detailed) but an intent to cause sexual arousal or titillation is present. It is evident that a mature sexual theme is being displayed or described.
**Spam messages** are unwanted, unsolicited e-mail messages received from an external address. Most spam messages are advertisements. However, some may be messages with criminal content, such as child pornography and scams.
**Subscriptions** are agreements to receive, participate or access mailing lists and newsgroups.
**Threat** is any potential event or act, deliberate or accidental, that could cause injury to employees or assets.
**Transitory information** is information that is required for a limited time to ensure the completion of a routine action or the preparation of a subsequent document. Transitory information includes information in a form used for casual communication, draft versions of documents where comments and additional information are incorporated into subsequent versions, process versions of documents that were not communicated outside the creating office, and duplicate versions of documents used as a reference source only.
**User account** includes all files, folders, e-mail messages or records of accesses to the Internet contained in an account assigned to a user or in a shared drive.
**Value** is estimated worth: monetary, cultural, intellectual or other.
**Violence** includes material where physically injurious or violent acts or treatment are being depicted.
**Virus** is a program that infects a computer by attaching itself to another program and propagating itself when that program is executed.
**Vulnerability** is an inadequacy related to security that could permit a threat to cause injury.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Politique sur l'utilisation des ressources électroniques

PROTECTION • SERVICE • INTÉGRITÉ





# 1. Date d'entrée en vigueur

Cette politique entre en vigueur dès sa diffusion.

Cette version de la politique remplace la version 1.1 (04 janvier 2011). Elle intègre des mises à jour de références ministérielles et définitions qui prennent effet le 13 mai 2013.

# 2. Politique

La politique de l'Agence des services frontaliers du Canada (ASFC) sur l'utilisation des ressources électroniques s'inspire de la Politique du Secrétariat du Conseil du Trésor sur l'utilisation acceptable des dispositifs et des réseaux.

# 3. Objectif de la politique

La présente politique a pour but de veiller à ce que les personnes qui ont accès aux systèmes et ressources électroniques de l'Agence, y compris les réseaux et systèmes électroniques partagés avec l'Agence du revenu du Canada (ARC), Services partagés Canada (SPC) et Citoyenneté et Immigration Canada (CIC), utilisent comme il se doit les ressources électroniques.

La politique vise aussi à informer tous les utilisateurs autorisés de leurs obligations et de leurs responsabilités relativement à l'utilisation appropriée des ressources électroniques de l'ASFC.

# 4. Application

La présente politique s'applique à toutes les personnes qui utilisent les ressources électroniques de l'ASFC.

# 5. Contexte

L'ASFC utilise toute une gamme de ressources électroniques dont des réseaux informatiques, des serveurs et des postes de travail, des ordinateurs autonomes, des périphériques, des mémoires, des appareils portatifs et d'autres dispositifs utilisés pour créer, recueillir, stocker, transmettre ou traiter l'information essentielle au fonctionnement et aux activités quotidiennes de l'ASFC. L'adoption et l'application d'un ensemble commun de politiques sont essentielles à l'efficacité, à l'efficience et à la sécurité des opérations.

L'ASFC est assujettie entre autres à deux politiques du Secrétariat du Conseil du Trésor (SCT) : la Politique sur la sécurité du gouvernement et la Politique sur l'utilisation acceptable des dispositifs et des réseaux.

Ces politiques définissent :

- l'accès aux réseaux électroniques du gouvernement du Canada, dans les locaux du gouvernement et à l'extérieur;







- les utilisations acceptables et inacceptables de ces ressources;
- les responsabilités de l'utilisateur et de la direction;
- les mesures correctrices ou disciplinaires et les processus de surveillance des réseaux.

Aux termes des politiques du SCT, les ministères fédéraux qui autorisent des personnes à utiliser les réseaux électroniques sont tenus d'adopter des politiques et des procédures pour garantir une utilisation appropriée de ces réseaux et de ces ressources. De plus, les ministères sont tenus de protéger la confidentialité, l'intégrité et la disponibilité des biens et de l'information liés à la technologie de l'information (TI) en prenant des précautions adéquates contre des menaces changeantes.

# 6. Définitions

**Accès**

L'entrée en communication avec une ressource électronique fournie par l'ASFC à des personnes autorisées ou l'utilisation de cette ressource. L'accès à de telles ressources peut se faire dans les locaux du gouvernement ou d'ailleurs. Cet accès permet le télétravail et l'utilisation à distance et peut également s'appliquer à des personnes autorisées qui utilisent les ressources électroniques fournies par l'ASFC à des fins personnelles limitées, en dehors des heures de travail, tel qu'il est prévu par la présente politique.

**Personnes autorisées**

Comprend les employés de l'ASFC, les entrepreneurs et d'autres personnes qui ont été autorisées par la direction à utiliser les ressources électroniques de l'ASFC.

**Ressources électroniques**

Groupes d'ordinateurs, de réseaux et systèmes, fonctions ou dispositifs électroniques attribués à des utilisateurs ou à des programmes. Les ressources comprennent Internet, les logiciels ou les dispositifs internes de l'ASFC ainsi que les dispositifs publics et privés externes à l'Agence. Sont également inclus tout le matériel, notamment les ordinateurs autonomes, les portables, les périphériques, les mémoires, les dispositifs sans fil, et tout autre support utilisé pour obtenir, stocker ou diffuser de l'information, etc. (par ex : clés USB, tablettes, téléphones intelligents, etc.). Nombre de dispositifs non informatiques, notamment les caméras numériques et les téléphones cellulaires, sont considérés comme des ressources électroniques aux termes de la présente politique, en raison de leur capacité de stockage et de diffusion de l'information. Les ressources électroniques, pour l'application de la présente politique, comprennent toujours les services d'infrastructure et de réseau assurés à l'ASFC par le SPC et l'ARC ainsi que les services de réseau entre l'ASFC et d'autres organisations gouvernementales.

**Surveillance**







Processus actif de vérification constante de l'activité dans les réseaux et les systèmes, pour déceler toute activité anormale, illicite, inappropriée, criminelle ou inhabituelle.

**Vérification**

Collecte et enregistrement de données sur les activités de l'utilisateur, y compris l'accès aux fichiers.

**Surveillance des ressources électroniques**

Toute mesure nécessitant l'enregistrement et l'analyse par la suite de données sur l'activité liée à une ressource électronique pour des raisons touchant les besoins opérationnels et pour évaluer le degré de conformité à la politique gouvernementale.

Pour obtenir d'autres définitions, vous pouvez consulter l'annexe « E » du présent document ou le lexique de la DGIST. (Entrez « sécurité informatique » pour obtenir que les définitions de la sécurité informatique)

# 7. Énoncé de la politique

L'Agence des services frontaliers du Canada a pour politique de permettre aux personnes autorisées d'utiliser les ressources électroniques pour mener les affaires de l'État. Ceci peut comprendre communiquer avec des fonctionnaires et le public, recueillir des renseignements utiles à leurs fonctions, selon le besoin de connaître ces renseignements, et maîtriser les techniques d'utilisation de ces ressources.

Les ressources électroniques fournies à l'ASFC ou par l'ASFC sont réservées aux activités de l'Agence. Une utilisation personnelle limitée, tel qu'il est prévu dans la présente politique, est autorisée sur les systèmes, notamment le courriel, les programmes de Microsoft Office ou Internet, à condition que cette utilisation soit conforme à toutes les politiques applicables de l'ASFC, ainsi que des politiques et lois applicables du gouvernement fédéral et des provinces. Toute l'information obtenue, stockée ou diffusée au moyen des ressources électroniques de l'ASFC et toutes les activités menées par les utilisateurs dans les systèmes sont assujetties à une surveillance. Dans le cadre de ses pratiques de surveillance, l'Agence respecte le droit des utilisateurs et des particuliers à la vie privée et maintient un équilibre raisonnable entre les attentes des utilisateurs en matière de vie privée et le devoir qu'a l'organisation de protéger l'information et les biens. Les incidents de sécurité seront signalés, et des enquêtes seront menées le cas échéant. Les documents informatiques sont assujettis aux exigences en matière d'accès à l'information et de protection des renseignements personnels (AIPRP) et peuvent faire l'objet de demandes connexes. Toute personne enfreignant la présente politique fera l'objet de mesures disciplinaires pouvant aller jusqu'au renvoi.

# 8. Exigences de la politique

Toutes les lois fédérales et les politiques fédérales régissant l'utilisation de ressources électroniques s'appliquent aux systèmes informatiques et aux ressources électroniques de l'ASFC.







Cette politique devrait être lue en accord avec la Directive sur l'utilisation appropriée du courrier Électronique (courriel) et la Directive relative à l'utilisation de la technologie sans fil.

Tout document électronique peut être consulté aux termes de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, sauf exceptions prévues dans ces lois.

# 9. Utilisation autorisée des ressources électroniques

Les ressources électroniques sont utilisées dans le cadre d'activités permettant d'exécuter le mandat et la mission de l'ASFC. Les personnes autorisées doivent utiliser uniquement les applications, le matériel et les logiciels autorisés par l'Agence et installés par du personnel de la TI autorisé par l'ASFC ou l'ARC.

Les ressources électroniques de l'ASFC sont réservées à des fins approuvées, soit :

a. Activités du gouvernement, par exemple :
    - échanger de l'information avec des collègues, d'autres organismes et ministères fédéraux et le secteur privé dans l'exécution des fonctions et des activités de l'ASFC;
    - effectuer des recherches pour les besoins de l'Agence;
    - recueillir de l'information pertinente dans le cadre des fonctions de l'utilisateur;
    - apprendre à utiliser les ressources électroniques plus efficacement;
    - mener des activités de perfectionnement professionnel liées aux fonctions du poste.

b. Utilisation personnelle limitée (pendant les pauses-repas, les périodes de repos ou avant ou après le travail, tel qu'il est précisé dans le Code de conduite de l'ASFC), par exemple :
    - communiquer avec des parents, amis et autres personnes, à d'autres fins que des fins officielles;
    - consulter des sources de nouvelles et d'information acceptables, qui ne sont pas interdites ni restreintes par la loi ou les politiques;
    - effectuer des transactions bancaires personnelles régulières;
    - toute activité syndicale expressément autorisée par écrit par le gestionnaire compétent.

c. Toute autre activité conforme à la Politique du Secrétariat du Conseil du Trésor sur l'utilisation acceptable des dispositifs et des réseaux et à la présente politique ou expressément autorisée par écrit par la direction.

## Conditions d'utilisation personnelle limitée

Une utilisation personnelle limitée, tel qu'il est prévu par la présente politique, est autorisée sur les systèmes, notamment les courriels, les programmes de Microsoft Office ou Internet, à







condition que cette utilisation soit conforme à toutes les politiques applicables de l'ASFC, ainsi que des politiques et lois applicables du gouvernement fédéral et des provinces. Tous les autres réseaux et toutes les autres ressources électroniques de l'ASFC sont réservés aux fins de l'Agence, et leur utilisation se limite aux activités directement liées aux fonctions officielles d'un utilisateur autorisé.

Cette utilisation personnelle limitée ne doit pas :

a. nuire à la productivité de l'utilisateur ni à l'exécution de ses fonctions officielles;
b. entraîner des coûts directs pour l'Agence;
c. faciliter une activité criminelle, illicite ou inacceptable, tel qu'il est indiqué dans la présente politique;
d. constituer un fardeau à l'égard du rendement ou de la capacité de stockage des ressources électroniques de l'Agence.

L'ASFC peut restreindre ou interdire toute utilisation de ses ressources électroniques et de ses réseaux si :

a. cette utilisation menace la capacité ou l'intégrité des réseaux électroniques, des ressources ou des ordinateurs de l'ASFC;
b. la restriction ou l'interdiction s'impose pour des raisons opérationnelles ou administratives.

## Courriel

Le courriel est un outil de communication professionnelle essentiel au fonctionnement quotidien et aux activités de l'Agence. L'utilisation du courriel de l'Agence pour des activités inacceptables ou illicites, notamment des affaires personnelles et commerciales ou pour aider des parents, des amis ou d'autres personnes à mener de telles activités, est strictement interdite. L'utilisation du courriel pour la transmission d'avis syndicaux ou d'autres documents syndicaux doit être approuvée par écrit par l'Agence.

Le courriel est assujetti à toutes les dispositions législatives régissant les communications écrites, dont la Loi sur l'accès à l'information, la Loi sur la protection des renseignements personnels, la Loi sur la Bibliothèque et les Archives du Canada,, la Loi sur les langues officielles, la Loi canadienne sur les droits de la personne, et le Code criminel. Aux termes de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, le public peut avoir accès aux documents électroniques, sous réserve des exceptions applicables prévues dans ces lois.

Pour en savoir plus au sujet du courriel, consultez la directive de l'ASFC sur l'utilisation appropriée du courriel .

## Renseignements organisationnels et transitoires (temporaires)







Toute information, y inclus le courriel, (sous forme matérielle ou électronique) créée, stockée, reçue ou transmise au moyen des ressources électroniques et qui contient des renseignements sur les fonctions, les mesures et les décisions de l'ASFC doit être conservée. Tous les utilisateurs doivent gérer efficacement toute l'information qu'ils créent et stockent. L'information doit être protégée contre la destruction et l'accès non autorisés. Pour en savoir plus sur les renseignements organisationnels (de l'organisation) et transitoires, consultez la Politique de la gestion de l'information (GI) de l'ASFC ainsi que la politique du Secrétariat du Conseil du Trésor sur Politique sur la gestion de l'information.

## 10. Utilisation non autorisée des ressources électroniques

Les ressources électroniques de l'ASFC ne doivent en aucun cas être utilisées pour exploiter des logiciels ou des applications non-autorisés, dont des jeux ou d'autres logiciels de divertissement, sauf avec l'autorisation expresse de l'ASFC[1]. Les utilisateurs ne doivent en aucun cas consulter l'information de l'ASFC à leur sujet ou au sujet de leurs collègues, de leurs parents ou amis ou de toute autre personne n'étant pas liée au travail, sauf lorsque la consultation de cette information est directement liée à un programme autorisé ou à une activité que la personne est expressément autorisée à exercer. Les systèmes et l'information de l'ASFC doivent être utilisés strictement sur la base du « besoin de connaître ». Cela signifie que l'accès à des renseignements et à des systèmes d'information précis n'est consenti qu'aux personnes autorisées qui ont la cote de sécurité requise, et ce, en fonction des exigences officielles propres à l'emploi occupé. L'accès aux renseignements est considéré privilégié et ceux-ci ne doivent pas être partagés, discutés ou divulgués à quiconque. Le droit d'accès des utilisateurs doit être révisé lorsque leurs fonctions ou leur statut change.

## 11. Activités criminelles, illicites et inacceptables

Il existe trois catégories d'activités inappropriées concernant les ressources électroniques : les activités criminelles, les activités illégales qui ne sont pas criminalisées et les activités inacceptables.

Les ressources électroniques de l'ASFC ne doivent pas être utilisées pour mener :

1. des activités criminelles (p. ex. pornographie juvénile, obscénité, droit d'auteur, diffamation, piratage, harcèlement, propagande haineuse);
2. des activités illégales qui ne sont pas criminalisées, y compris les infractions aux lois et règlements fédéraux et provinciaux et les gestes qui exposent une personne autorisée ou l'Agence à des poursuites civiles (p. ex. destruction de données, divulgation de renseignements délicats, diffusion de renseignements erronés);
3. des activités qui, bien que licites, sont inacceptables et enfreignent les politiques de l'Agence ou du Conseil du Trésor (p. ex. transmettre de l'information classifiée dans les réseaux non protégés, transmettre des messages insultants, sexistes ou racistes, présenter ses opinions personnelles comme étant celles de l'ASFC).







S'il existe des motifs raisonnables de soupçonner une utilisation criminelle, ilicite ou inacceptable des ressources électroniques, de telles activités doivent être signalées au gestionnaire compétent.[2]

La liste non exhaustive de ces activités figure aux annexes « A », « B » et « C ». D'autres exemples d'utilisation abusive sont mentionnés à l'annexe « D ».

---

[1] Les appareils électroniques personnels, par exemple, un ordinateur à domicile, téléphones intelligents, tablettes, etc., ne doivent pas être utilisés pour traiter l'information de l'ASFC. Les employés ne doivent pas brancher leurs appareils électroniques personnels à l'équipement informatique de l'ASFC, par exemple, le chargement d'un appareil personnel à partir d'un port USB.

[2] Nota : Les employés autorisés peuvent devoir consulter des sites à accès limité, notamment des sites de matériel pornographique ou de propagande haineuse, dans le cadre d'enquêtes autorisées ou de collecte de renseignements et pour étudier ou mettre au point des documents autorisés par l'ASFC, par exemple des documents de formation. Les employés de l'ASFC peuvent devoir consulter tous les types de documents pour tirer des conclusions concernant l'admissibilité.

# 12. Rôles et responsabilités

## Personnes autorisées

Quiconque a accès aux ressources électroniques de l'ASFC doit respecter la présente politique ainsi que toutes les politiques et lois applicables du gouvernement et sera tenu responsable de toutes les activités menées au moyen des ressources électroniques de l'ASFC.

Les utilisateurs autorisés doivent se familiariser avec la présente politique et la respecter chaque fois qu'ils utilisent les réseaux et ressources électroniques de l'Agence.

Les personnes autorisées sont tenues d'utiliser les ressources électroniques de l'ASFC de façon appropriée, par exemple :

a. s'assurer que des mesures approuvées sont prises pour contrôler l'utilisation de leurs mots de passe, de leur nom d'utilisateur ou de leurs comptes informatiques, par exemple en évitant de communiquer cette information;
b. signaler les cas d'utilisation abusive, inacceptable ou illicite telle que les chaînes de lettres, les virus informatiques;
c. connaître les politiques sur la sécurité des technologies de l'information et tous les problèmes signalés par le dirigeant principal de l'information (DPI) ou l'agent de sécurité du ministère (ASM);
d. utiliser les dispositifs de sécurité informatique (chiffrement, programme antivirus) fournis par l'ASFC, au besoin;
e. communiquer de façon à ne pas jeter le discrédit sur le mandat et la mission de l'ASFC;







f. obtenir des précisions du directeur de la sécurité informatique et de la continuité informatique et de l'agent de la sécurité du ministère en cas de doute quant au caractère acceptable ou licite d'une utilisation planifiée, conformément à la politique.

## Gestionnaires

Les gestionnaires doivent :

a. déterminer et approuver l'accès des utilisateurs à des systèmes précis;
b. informer les utilisateurs de leurs responsabilités relativement à l'utilisation appropriée des ressources électroniques de l'ASFC;
c. signaler les cas suspects d'utilisation criminelle, illicite ou inacceptable des ressources électroniques de l'ASFC à la Direction de la sécurité et des normes professionnelles,
d. gérer rapidement, de façon équitable et décisive, les infractions à la politique ou à la loi;
e. s'assurer qu'aucun renseignement organisationnel ne reste sur le lecteur réseau personnel de l'utilisateur à son départ (p. ex. retraite, détachement, affectation).

## Directeur général, Direction des services d'infrastructure

Le directeur général des Services d'infrastructure doit :

a. fournir la formation ou l'information nécessaires à l'utilisation efficace des ressources électroniques;
b. établir les procédures régissant l'accès aux ressources électroniques de l'ASFC;
c. établir les procédures, en collaboration avec le directeur général de la Direction de la sécurité et des normes professionnelles ou l'ASM, régissant l'accès à Internet au moyen des ressources électroniques de l'ASFC.

## Agent de sécurité du ministère (ASM)

L'agent de sécurité du ministère doit :

a. fournir des précisions sur la présente politique;
b. fournir de l'information sur l'interprétation des utilisations licites et acceptables des ressources électroniques de l'ASFC;
c. approuver les personnes autorisées à surveiller l'utilisation des ressources électroniques;
d. renvoyer les gestionnaires à la Direction de la sécurité et des normes professionnelles pour les questions d'accès aux courriels ou aux fichiers contenus dans un compte d'utilisateur;





e. renvoyer les gestionnaires à la Direction de la sécurité et normes professionnelles lorsqu'une utilisation abusive des ressources électroniques de l'Agence est soupçonnée;
f. enquêter sur les rapports faisant état de cas suspects d'activités criminelles, illicites ou inacceptables menées grâces aux ressources électroniques de l'ASFC;
g. demander conseil au Service des relations de travail et aux Services juridiques en cas d'utilisation criminelle ou illicite soupçonnée des ressources électroniques de l'ASFC et s'adresser aux autorités chargées de l'application de la loi, le cas échéant;
h. répondre à toute demande relative à la Loi sur l'accès à l'information qui se rapporte à l'application de cette politique.

## Personnel opérationnel des TI

Sous la direction générale du coordonnateur de la sécurité des TI et conformément aux priorités, politiques et procédures de l'Agence, le personnel opérationnel des TI doit :

a. comprendre et respecter les politiques et procédures de sécurité des TI de l'ASFC pour protéger les opérations et les infrastructures des TI;
b. donner suite aux incidents de sécurité et les signaler à leur gestionnaire compétent et ensuite directement à la Direction de la sécurité et des normes professionnelles [2]
c. mettre à l'essai et installer des rustines de sécurité conformément aux procédures approuvées de l'Agence;
d. entretenir ou mettre à niveau le matériel et les logiciels et contrôler la configuration de l'infrastructure en appliquant de saines pratiques de gestion de la configuration et de contrôle des changements.

---

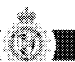
[2] En cas d'utilisation abusive soupçonnée des ressources électroniques de l'Agence, le personnel opérationnel des TI n'est pas autorisé, sans approbation, à prendre des mesures immédiates, pour éviter toute répercussion négative sur une éventuelle enquête.

# 13. Protection de la vie privée et surveillance

## Attentes en matière de protection de la vie privée

La politique du gouvernement sur la sécurité reconnaît que :

a. la Charte canadienne des droits et libertés garantit que les personnes autorisées par le gouvernement peuvent avoir des attentes raisonnables à cet égard en milieu de travail;
b. les personnes autorisées sont également protégées par la Loi sur la protection des renseignements personnels, et que certaines



limites s'appliquent aux responsables de l'organisation en ce qui concerne la fouille des employés et de leurs effets.

L'ASFC doit également protéger la vie privée des particuliers en ce qui a trait aux renseignements personnels les concernant conformément à la Loi sur la protection des renseignements personnels et la Loi sur les douanes (articles 107 et 160).

## Surveillance des ressources électroniques

Un des objectifs de la surveillance est d'encourager les utilisateurs à respecter la présente politique. De plus, les pratiques de surveillance de l'Agence respectent le droit à la vie privée des employés et des particuliers et garantissent un équilibre raisonnable entre vie privée et devoir de protection de l'information et des biens de nature délicate (dont les ressources électroniques), et l'Agence mène ses activités avec efficacité dans le respect de la loi.

L'ASFC effectue trois types de surveillance, qui sont décrits ci-dessous :

### 1. Surveillance opérationnelle

La Direction des services d'infrastructure est responsable de la surveillance des ressources électroniques pour des motifs opérationnels. Son but est de déterminer si les ressources fonctionnent efficacement, de cerner et de régler les problèmes et d'évaluer la conformité à la politique gouvernementale. En outre, des vérifications périodiques et aléatoires des ressources, à des fins opérationnelles précises, peuvent survenir, et l'information ainsi recueillie peut être analysée.

L'analyse ordinaire ne comprend pas la lecture du contenu des courriels, des fichiers ni des transmissions.

La surveillance peut comprendre :

a. déterminer la taille et le type des fichiers soupçonnés de causer des difficultés;
b. déterminer les habitudes d'utilisation;
c. déterminer l'expéditeur, le destinataire et l'objet des courriels;
d. détecter les virus;
e. effectuer des recherches par mot clé dans les fichiers stockés dans les ressources électroniques, y compris les serveurs de réseau et les dispositifs de stockage informatique;
f. repérer les codes malveillants et les activités illégales, illicites, inhabituelles ou inacceptables.

### 2. Surveillance du contenu



La Direction de la sécurité et des normes professionnelles est responsable de la surveillance du contenu des courriels et des fichiers d'un utilisateur. Le réseau électronique de l'ASFC consigne automatiquement l'identité des personnes et leurs activités alors qu'elles sont dans le réseau.

Des copies des fichiers et des courriels (y compris les documents supprimés) peuvent être consultées aux termes de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, sauf exceptions prévues dans ces lois.

## 3. Surveillance des activités illicites et des comportements inacceptables

Si, par suite d'une analyse ordinaire ou d'une plainte, il y a un motif raisonnable de soupçonner qu'une personne fait une utilisation abusive des ressources électroniques de l'Agence, la question est renvoyée à la Direction de la sécurité et des normes professionnelles pour enquête. Celle-ci peut autoriser la surveillance sans préavis, y compris la lecture ou l'examen du contenu des courriels ou des fichiers de l'intéressé. Si l'on constate qu'un abus des ressources électroniques a eu lieu, voir la section des « Mesures disciplinaires » de la présente politique.

# 14. Enquêtes

Les personnes autorisées qui doivent consulter le contenu des communications et des documents électroniques dans le cadre d'une enquête sont tenues par la loi de respecter le caractère confidentiel des renseignements et de les utiliser uniquement aux fins autorisées. Les enquêtes doivent être menées en conformité avec la Charte canadienne des droits et libertés, la Loi sur la protection des renseignements personnels, le Code criminel et les procédures de l'ASFC relatives aux enquêtes internes.

# 15. Mesures disciplinaires

Après consultation avec les Relations de travail et ses conseillers juridiques, l'ASFC signale aux autorités chargées de l'application de la loi les utilisations illicites et criminelles qui semblent être faites de ses ressources électroniques.

L'ASFC prend des mesures disciplinaires en cas d'utilisation illicite, criminelle ou inacceptable de ses ressources électroniques. Les mesures disciplinaires sont proportionnelles à la gravité et aux circonstances de l'incident.

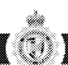
Les mesures disciplinaires peuvent comprendre :

a. une réprimande verbale ou écrite;
b. l'imposition de restrictions de l'accès aux ressources électroniques;
c. une suspension ou un renvoi.

Les mesures disciplinaires qui peuvent être prises à l'encontre des entrepreneurs et d'autres personnes autorisées à utiliser les ressources électroniques de l'ASFC sont précisées dans un accord sur les conditions d'utilisation annexé au contrat.







Pour de plus amples renseignements concernant les mesures disciplinaires, voir le Code de conduite, de l'ASFC, le document intitulé Politique de l'ASFC en matière de discipline, Lignes directrices en matière de discipline et toutes les autres politiques et lignes directrices applicables.

# 16. Examen de la politique

Cette politique doit être revue au moins aux cinq ans, sous l'autorité du directeur général de la Direction des services d'infrastructure, et du directeur général de la Direction de la sécurité et des normes professionnelles, ainsi que de l'agent de sécurité du ministère (ASM).

# 17. Références

## Lois et politiques pertinentes

Code de conduite de l'ASFC
Politique de l'ASFC en matière de discipline et Lignes directrices en matière de discipline
Code de valeurs et d'éthique du secteur public
Loi sur les douanes, article 107
Explication de l'article 107 de la Loi sur les douanes
Loi sur la gestion des finances publiques
Loi sur l'accès à l'information
Loi sur la protection des renseignements personnels
Charte canadienne des droits et libertés
Loi sur la Bibliothèque et les Archives du Canada
Loi sur la protection de l'information
Code criminel
Loi sur les licences d'exportation et d'importation
Loi sur la responsabilité civile de l'État et le contentieux administratif
Loi sur le droit d'auteur
Loi sur les marques de commerce
Loi sur les brevets
Loi canadienne sur les droits de la personne
Loi sur les langues officielles

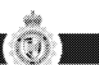
## Autres documents pertinents

## Politiques et publications du Conseil du Trésor

Lignes directrices concernant la discipline
Politique sur la prévention et résolution du harcèlement en milieu de travail
Politique sur la sécurité du gouvernement
Politiques sur les communications gouvernementales
Politique sur la gestion de l'information
Gestion de la sécurité des technologies de l'information (GSTI)







Politique sur l'accès à l'information
Accès à l'information et protection des renseignements personnels
Politique sur l'utilisation acceptable des dispositifs et des réseaux
Politique de télétravail
Directive sur les pertes de fonds et de biens

## 18. Demandes de renseignements

Les demandes de renseignements concernant cette politique doivent être présentées aux bureaux suivants :
**Direction générale, Information, sciences et technologie**
Coordonnateur de la STI, Sécurité et continuité de la TI :
Courriel : CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca
Intranet: Sécurité de la TI

**Direction générale du contrôle**
Direction de la sécurité et des normes professionnelles
Courriel : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca







# Annexe A

## Actes criminels

**(Liste d'exemples non exhaustive)**

Voici des exemples d'activités criminelles qui pourraient être menées à l'aide des réseaux et des ressources électroniques.

a. **Pornographie juvénile :** Avoir en sa possession, télécharger ou distribuer de la pornographie juvénile (voir l'article 163.1 du Code criminel).
b. **Droit d'auteur :** Porter atteinte au droit d'auteur d'autrui sans raison licite - la Loi sur le droit d'auteur prévoit des poursuites au pénal et au civil en pareils cas (voir également la section sur le droit d'auteur à la rubrique portant sur les infractions à des lois fédérales et provinciales).
c. **Diffamation :** Faire lire par d'autres personnes un énoncé susceptible de nuire à la réputation de quelqu'un en l'exposant à la haine, au mépris ou au ridicule, ou conçu pour l'insulter (voir les articles 296 à 317 du Code criminel).
d. **Piratage et autres crimes contre la sécurité informatique - Accès non autorisé à un système informatique :** Utilisation du mot de passe ou des codes de cryptage d'autrui pour commettre une fraude ou obtenir de l'argent, des biens ou des services en faisant de fausses représentations sur un système informatique. Voir les articles suivants du Code criminel : 122 (abus de confiance par un fonctionnaire public); 380 (fraude); 361 (escroquerie); 403 (supposition frauduleuse de personne); 342.1 (utilisation non autorisée d'ordinateur et de services informatiques).
e. **Tentative de percer les dispositifs de sécurité des réseaux électroniques :** Voir les dispositions suivantes du Code criminel : 342.1 (utilisation non autorisée d'ordinateur et de services informatiques); alinéa 342.1d) (utilisation, possession ou trafic de mots de passe d'ordinateur volés ou de renseignements relatifs à des cartes de crédit volées); article 342.2 (production, possession ou distribution de programmes informatiques conçus pour faciliter l'accès illégal à des systèmes informatiques); articles 429 et 430 (méfait concernant des données).
f. **Introduction de virus dans l'intention de causer du tort :** Voir les articles suivants du Code criminel : 429 et 430 (méfait concernant des données) ainsi que 342.1 (utilisation non autorisée d'ordinateur et de services informatiques).
g. **Destruction, modification ou cryptage de données sans autorisation, dans l'intention d'en interdire l'accès à d'autres en ayant licitement besoin :** Voir les dispositions suivantes du Code criminel : articles 429 et 430 (méfait concernant des données); article 342.1 (utilisation non autorisée d'ordinateur et de services informatiques); article 129 et paragraphe 139(2) (destruction ou falsification de preuves pour faire obstacle à une enquête pénale).
h. **Entrave à l'utilisation licite par d'autres de données et d'ordinateurs :** Voir les articles suivants du Code criminel : 429 et 430 (méfait concernant des données); 326 (vol de service de télécommunication); 322 (vol d'équipement informatique); 342.1 (utilisation non autorisée d'ordinateur et de services informatiques).
i. **Harcèlement :** Envoyer, sans en avoir l'autorité légale, des messages électroniques incitant quelqu'un à craindre pour sa sécurité ou pour celle de gens qu'il connaît (voir l'article 264 du Code criminel). Selon l'article 264.1 du Code criminel, commet une







infraction quiconque fait parvenir à autrui des menaces de lui causer des lésions corporelles, d'endommager ses biens ou de blesser un animal qui lui appartient.

j. **Propagande haineuse :** Diffuser ou distribuer des messages fomentant la haine ou incitant à la violence contre des groupes identifiables autrement que dans une conversation privée (voir l'article 319 du Code criminel).
k. **Interception de communications privées ou de courrier électronique (en transit) :** Intercepter illégalement les communications privées de quelqu'un ou intercepter illégalement le courrier électronique de quelqu'un (voir respectivement les articles 184 et 342.1 du Code criminel).
l. **Obscénité :** Distribuer, publier ou avoir en sa possession en vue de le distribuer ou de l'exposer publiquement tout document obscène (p. ex. représentation d'actes sexuels explicites exploitant indûment la sexualité, accompagnés de violence ou avec la participation ou en présence d'enfants, ou encore d'actes sexuels dégradants ou déshumanisants, entraînant un risque réel que le document incite d'autres personnes à se livrer à des actes antisociaux) (voir l'article 163 du Code criminel).
m. **Divers autres crimes :** Le Code criminel et quelques autres lois prévoient toute une gamme d'autres actes criminels susceptibles d'être entièrement ou partiellement commis grâce à l'utilisation des réseaux informatiques. Par exemple, la fraude, l'extorsion, le chantage, la corruption, les paris illégaux et le trafic de drogues illégales sont tous des actes criminels qui peuvent être commis, du moins en partie, sur les réseaux électroniques.



# Annexe B

## Activités illicites qui enfreignent des lois fédérales ou provinciales

### (Liste d'exemples non exhaustive)

Voici des exemples d'activités illégales (mais non criminelles) susceptibles d'être menées sur les réseaux et au moyen de ressources électroniques.

a. **Atteintes au droit d'auteur et à la propriété intellectuelle :** Violation du droit d'auteur (la Loi sur le droit d'auteur prévoit des poursuites au pénal et au civil en pareils cas). Il se peut que des marques de commerce et des brevets soient utilisée sans autorisation sur les réseaux électroniques, en contravention de la Loi sur les marques de commerce.
b. **Diffamation :** Fait de répandre des allégations ou des rumeurs mensongères nuisant à la réputation d'autrui. En plus d'être un acte criminel, la diffamation est interdite par les lois provinciales.
c. **Destruction ou modification de données sans autorisation :** Destruction, modification ou falsification illégale de documents électroniques. Voir l'article 5 de la Loi sur les Archives nationales du Canada, les articles 6 et 12 de la Loi sur la protection des renseignements personnels, l'article 4 de la Loi sur l'accès à l'information et l'article 5 de la Loi sur les secrets officiels.
d. **Communication non autorisée de données délicates – Communication de renseignements personnels :** le fait de ne pas respecter la vie privée et la dignité d'un individu. L'obligation de respecter la vie privée d'une personne est exprimée dans plusieurs dispositions législatives, comme les articles 4, 5, 7 et 8 de la Loi sur la protection des renseignements personnels et le paragraphe 19(1) de la Loi sur l'accès à l'information. De nombreuses lois fédérales contiennent des dispositions interdisant la communication de renseignements de ce genre, souvent dans le but de protéger la vie privée des citoyens qui fournissent des renseignements au gouvernement (voir la liste de ces dispositions à l'Annexe II de la Loi sur l'accès à l'information). Le Code civil et la Charte des droits de la personne du Québec contiennent plusieurs dispositions analogues (les articles 3 et 35 à 41 et les articles 4, 5 et 49, respectivement). La Colombie-Britannique, la Saskatchewan, le Manitoba et Terre-Neuve-et-Labrador ont aussi des lois qui prévoient des poursuites au civil en cas d'atteinte injustifiée à la vie privée.
e. **Divulgation de secrets industriels :** Révélation non autorisée de secrets industriels, ou en réponse à une demande officielle présentée en vertu de la Loi sur l'accès à l'information, de secrets industriels ou de renseignements commerciaux confidentiels communiqués à titre confidentiel par un tiers et traités comme







tels de façon constante par celui-ci. Voir les alinéas 20(1)a) et b) de la Loi sur l'accès à l'information.

f. **Divulgation de renseignements gouvernementaux de nature délicate :** Communication non autorisée de renseignements gouvernementaux de nature délicate; voir les articles 3 et 4 de la Loi sur les secrets officiels. Par ailleurs, lorsqu'elles répondent à des demandes officielles présentées en vertu de la Loi sur l'accès à l'information, les organisations fédérales ne doivent pas communiquer de renseignements reçus à titre confidentiel d'autres gouvernements (voir l'article 13 de la Loi sur l'accès à l'information). Les autres exceptions prévues à cet égard dans la Loi sont de nature discrétionnaire. Il convient de souligner que les fonctionnaires et autres personnes autorisées ainsi que le gouvernement ne peuvent pas être poursuivis en justice à l'égard des communications qu'ils ont faites de bonne foi aux termes soit de la Loi sur la protection des renseignements personnels, soit de la Loi sur l'accès à l'information.
g. **Harcèlement :** Constitue un acte discriminatoire, « s'il est fondé sur un motif de distinction illicite, le fait de harceler un individu : a) lors de la fourniture [...] de services [...] destinés au public; [...] c) en matière d'emploi ». Les motifs de distinction illicite sont ceux qui sont fondés sur la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, l'orientation sexuelle, l'état matrimonial, la situation de famille, la déficience ou l'état de personne graciée. Ainsi, dans certaines circonstances, afficher des images sexistes, pornographiques, racistes ou homophobes indésirables au travail, sur un écran d'ordinateur, peut constituer du harcèlement. Voir l'article 14 de la Loi canadienne sur les droits de la personne.
h. **Atteintes à la vie privée :** Lecture du courrier électronique ou d'autres renseignements personnels d'autrui sans autorisation, écoute des conversations privées ou interception du courrier électronique en transit, par exemple.
i. Un fonctionnaire ou une autre personne peut avoir des attentes raisonnables quant au caractère privé des renseignements contenus dans son courrier électronique ou dans d'autres documents personnels, l'organisation - qu'elle agisse à titre d'employeur ou autrement - peut être coupable d'une infraction à l'article 8 de la Charte canadienne des droits et libertés (perquisitions et saisies abusives) si, en l'absence d'une autorité légale, elle ne respecte pas ces attentes raisonnables.
j. L'organisation peut aussi être réputée avoir recueilli ou utilisé illégalement des données en contravention des articles 4, 5, 7 et 8 de la Loi sur la protection des renseignements personnels. Le gouvernement peut être passible de poursuites en dommages-intérêts quand des communications privées sont interceptées illégalement (voir les articles 16 à 20 de la Loi sur la responsabilité civile de l'État et le contentieux administratif, sur les activités de surveillance électronique exécutées par des fonctionnaires dans le cadre de leurs fonctions. L'article 20





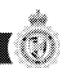
dispose expressément que le fonctionnaire est redevable envers l'État du montant des dommages-intérêts accordé par un tribunal). Le gouvernement peut aussi s'exposer à des poursuites en dommages-intérêts quand une communication illégale de renseignements personnels a lieu en contravention des dispositions de diverses lois (voir la liste de ces dispositions à l'Annexe II de la Loi sur l'accès à l'information). Pour un complément d'information sur ces questions, voir l'Annexe E, qui contient un exposé sur les attentes raisonnables quant à la protection de la vie privée.

k. **Utilisation des deniers publics sans autorisation :** Voir les articles suivants de la Loi sur la gestion des finances publiques : 33 (demande de paiement non autorisée); 34 (attestation non autorisée de livraison de fournitures ou de prestation de services); 78 (responsabilité des pertes résultant d'une malversation ou d'une négligence); 80 (acceptation de pots-de-vin ou participation à des activités de corruption).

## Activités pouvant exposer des personnes autorisées ou l'employeur à des poursuites en responsabilité civile

Divers comportements peuvent exposer une personne autorisée ou un employeur à des poursuites en responsabilité civile. L'employeur est réputé responsable lorsqu'un fonctionnaire se livre à une activité illégale dans le cadre de ses fonctions. Le fonctionnaire peut être tenu personnellement responsable de ses actes, mais le gouvernement fédéral en est lui aussi responsable. (La politique gouvernementale d'indemnisation des personnes autorisées, qui s'intitule Politique sur l'immunité accordée aux fonctionnaires de l'État, est pertinente dans ce contexte.) Voici des exemples de quasi-délits civils susceptibles de se produire sur les réseaux électroniques.

a. **Communication ou collecte de données de nature délicate :** Révéler ou obtenir de tels renseignements sans autorisation. En plus des dispositions législatives déjà mentionnées, la communication ou la collecte non autorisées de renseignements personnels peut donner lieu, dans certaines circonstances, à des poursuites au civil pour atteinte à la vie privée, nuisance ou intrusion common law et à des poursuites analogues fondées sur le Code civil du Québec (articles 3 et 15 à 41), pour rupture de contrat ainsi que pour abus de confiance (p. ex. si des renseignements commerciaux confidentiels sont communiqués).
b. **Diffamation :** Répandre des allégations ou des rumeurs mensongères susceptibles de porter atteinte à la réputation de quelqu'un. Outre qu'il s'agit d'un acte criminel, la publication de déclarations diffamatoires sans défense légale peut exposer son auteur à des poursuites au civil.
c. **Communication de renseignements erronés :** Afficher des renseignements erronés, par négligence ou à dessein. Ce genre de comportement peut donner lieu à des poursuites au civil pour assertion négligente et inexacte si l'on peut démontrer : a) que



l'affichage a lésé une personne et porté préjudice à une personne qui b) s'était raisonnablement fondée sur les renseignements, c) que la personne ou l'organisation qui a affiché les renseignements avait une obligation de prudence à l'égard de la personne lésée par les faux renseignements et d) que les erreurs étaient attribuables à la négligence (un comportement ne répondant pas aux critères de diligence raisonnable dans les circonstances).






# Annexe C

## Activités inacceptables qui, sans être nécessairement illégales, sont incompatibles avec les politiques du Conseil du Trésor ou de l'ASFC

**(Liste d'exemples non exhaustive)**

Un certain nombre de politiques du Conseil du Trésor ne s'appliquent pas à un moyen de communication plutôt qu'à un autre. En effet, elles sont aussi valables, que l'activité inacceptable se fasse par écrit, au téléphone, sur les réseaux informatiques, dans une conversation ou à l'aide d'un autre moyen de communication. Il est inadmissible qu'un fonctionnaire enfreigne les politiques du Conseil du Trésor et celles de l'ASFC, y compris les politiques organisationnelles. Les politiques suivantes sont importantes dans le contexte de l'utilisation des ressources informatiques : Politique sur la sécurité du gouvernement (relativement aux normes, y compris la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI); la Politique sur la prévention et le règlement du harcèlement en milieu de travail; la Politique sur la protection des renseignements personnels, y compris le Code de la protection des renseignements personnels concernant les employés; la Politique de communication du gouvernement; le Code de valeurs et d'éthique de la fonction publique; le Code de conduite de l'ASFC. Ces textes s'appliquent aux activités suivantes.

a. **Communiquer des renseignements protégés ou désignés sur des réseaux non protégés,** sauf s'ils sont chiffrés (Politique du gouvernement sur la sécurité; présente politique de l'ASFC).
b. **Consulter sans autorisation des renseignements délicats détenus par le gouvernement** (Politique du gouvernement sur la sécurité).
c. **Tenter de percer les dispositifs de sécurité des systèmes informatiques,** notamment en utilisant des programmes antisécurité, en se servant du mot de passe, du code d'utilisateur ou du compte informatique de quelqu'un d'autre, en donnant son mot de passe, des renseignements sur la configuration du réseau ou des codes d'accès à quelqu'un d'autre ou en désactivant des programmes antivirus (Politique du gouvernement sur la sécurité).
d. **Congestionner et perturber les réseaux et les systèmes,** notamment en envoyant des chaînes de lettres et en recevant du courrier électronique de serveurs de listes pour d'autres fins que le travail. Ce ne sont là que deux exemples d'utilisation abusive des ressources à des fins personnelles (Politique du gouvernement sur la sécurité).
e. **Envoyer des messages abusifs, sexistes ou racistes à des fonctionnaires ou à d'autres personnes** (Prévention et règlement du harcèlement en milieu de travail).
f. **Utiliser les réseaux électroniques du gouvernement pour des affaires commerciales personnelles, à des fins de gain**





**ou de profit personnel ou pour des activités politiques** Politique du SCT sur l'utilisation des réseaux électroniques).

g. **Faire publiquement des critiques excessives de la politique gouvernementale** (Code de conduite de l'ASFC; Code de valeurs et d'éthique de la fonction publique).

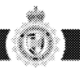
h. **Présenter ses opinions personnelles comme étant celles de l'organisation ou manquer autrement au devoir de se conformer aux procédures organisationnelles sur les déclarations publiques au sujet des positions du gouvernement** (Code de conduite de l'ASFC; Code de valeurs et d'éthique de la fonction publique).

i. **Manquer au devoir d'aviser les fonctionnaires et d'autres personnes autorisées des pratiques de surveillance et de vérification électroniques** (Politique du gouvernement sur la sécurité; Code de la protection des renseignements personnels concernant les employés).

j. **Donner accès aux systèmes, aux réseaux ou aux applications utilisées pour le traitement de renseignements délicats à du personnel n'ayant pas encore fait l'objet d'une enquête de sécurité adéquate** Politique du gouvernement sur la sécurité).

k. **Négliger d'annuler les droits d'accès aux systèmes lorsqu'un membre du personnel quitte l'organisation en raison d'une mise en disponibilité, à l'expiration d'un contrat ou à la suite de la perte de sa cote de fiabilité ou de son attestation de sécurité** (Politique du gouvernement sur la sécurité).

l. **Installer ou retirer sans autorisation du matériel ou des logiciels sur des ordinateurs ou des réseaux électroniques de l'État** (Politique du gouvernement sur la sécurité).

# Annexe D

## Autres exemples d'utilisation abusive des ressources électroniques de l'ASFC

Toutes les activités suivantes sont considérées comme une violation de la présente politique et peuvent entraîner des mesures disciplinaires.

Les utilisations inacceptables des ressources électroniques de l'Agence comprennent, sans en exclure d'autres, le fait d'obtenir, de stocker ou de transmettre de l'information dans les contextes suivants ou d'être complice de telles utilisations :

- Chaînes de lettres, opérations pyramidales, matériel de mauvais goût ou contenant des éléments pornographiques, de la nudité, des jurons, de la violence ou des aspects sexuels;
- Paris illégaux;
- Divulgation de son mot de passe, de son nom d'utilisateur ou d'autres renseignements de ce genre;
- Documents relatifs à la promotion ou à l'utilisation de substances illégales;
- Tentative en vue de désactiver des fonctions des technologies de l'information, grâce par exemple à des programmes antisécurité, à l'utilisation du mot de passe, de l'identité ou des comptes de réseau d'autrui, divulgation de mot de passe ou retrait ou modification de dispositifs de sécurité installés;
- Utilisation des réseaux électroniques de l'Agence pour faire des transactions personnelles, à des fins de gain ou de profit personnel ou pour des activités politiques;
- Transmission de propagande haineuse (peut aussi être une activité criminelle);
- Participation à des activités de jeu non autorisées, à des fins de profit personnel;
- Souscription à des listes d'envoi, à des groupes de discussion et à des salons de clavardage qui ne se rapportent pas à l'exécution des fonctions;
- Installation, stockage, utilisation, modification ou transmission de jeux, de logiciels non autorisés, de fichiers script ou de fichiers de données;
- Installation ou retrait de logiciels ou de matériel ou modification de leurs fonctions, sauf pour les membres du personnel opérationnel des TI autorisés à effecteur l'entretien de ces éléments;
- Installation d'économiseurs d'écran sans l'autorisation préalable du personnel opérationnel des TI;
- Fait de ne pas prendre les mesures antivirus voulues.


Agence des services frontaliers du Canada | Canada Border Services Agency



# Annexe E

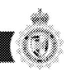
## Termes et définitions

L'Annexe E présente par ordre alphabétique les termes utilisés dans la Politique sur l'utilisation des ressources électroniques de l'ASFC, pour aider les utilisateurs à mieux comprendre les dispositions de la politique.

**Abonnements :** Accords concernant la réception ou l'utilisation de listes d'envoi et la participation aux activités de groupes de discussion. (Subscriptions)
**Activités privées :** Toute activité qui ne s'inscrit pas dans le cadre du travail et qui est menée à des fins d'avantages personnels. Cela comprend la vente ou l'achat de biens ou de services ainsi que les activités politiques. (Private business)
**Administration du contenu :** Peut comprendre l'installation de messages d'absence ou l'extraction de documents ministériels. (Content administration)
**Atteinte à la sécurité :** Compromission d'un actif ou tout acte ou omission qui pourrait mener à une compromission, à une menace ou à un acte de violence à l'endroit des employés. (Security incident)
**Biens :** Éléments d'actif, corporels ou incorporels, du gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale. (Assets)
**Chaînes de lettres :** Courriels qui n'ont qu'un seul but - vous inciter à les envoyer à d'autres. Ils vous promettent faussement de la chance, de l'argent ou la réalisation d'un souhait, à condition que vous les fassiez suivre. (Chain letters)
**Compromission :** Comprend les préjudices causés par la divulgation, la destruction, la suppression ou la modification non autorisées d'information ou par l'interruption ou l'utilisation non autorisées des biens. (Compromise)
**Compte d'utilisateur :** Tous les fichiers, les répertoires, les courriels ou les documents d'accès à Internet qui se trouvent dans un compte attribué à un utilisateur ou sur une unité partagée. (User account)
**Confidentialité :** Caractère de l'information qui ne doit pas être communiquée à des personnes non autorisées, en raison du tort que cela pourrait causer à l'intérêt national ou à d'autres intérêts, en conformité avec des dispositions précises de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels. (Confidentiality)
**Contenu à caractère sexuel :** Matériel qui ne présente pas nécessairement d'actes sexuels explicites mais qui vise à







provoquer une excitation sexuelle. Il est évident qu'un thème sexuel pour public averti est présenté ou décrit. (Sexual content)
**Disponibilité :** Fait de pouvoir être utilisé sur demande pour appuyer les opérations, les programmes et les services. (Availability)
**Documents :** Information sous forme matérielle ou électronique, y compris les documents audio-visuels, les photographies, les cartes, les dessins, les films, les enregistrements sonores, les bandes vidéo, les microformes, les bandes magnétiques, les imprimés, les fichiers électroniques et tout autre type de document. (Records)
**Document offensant :** Document qui risque d'insulter, de dégoûter ou d'offenser, y compris les blagues au sujet de certains groupes (p. ex. les blagues à caractère raciste, religieux ou sexiste). Il peut aussi s'agir d'images offensantes (p. ex. des images de cadavres, des représentations scatologiques). (Offensive material)
**Hameçonnage :** Forme de fraude par Internet qui utilise des courriels, des sites Web ou d'autres types d'information apparemment authentiques mais qui sont faux, pour subtiliser des renseignements précieux comme les numéros de carte de crédit ou d'assurance sociale, les identificateurs d'utilisateur et les mots de passe. (Phishing)
**Intégrité :** Caractère exact et complet des actifs et authenticité des transactions. (Integrity)
**Jeu :** Fait de parier ou de risquer de l'argent ou un objet de valeur dans un jeu de hasard ou un jeu qui combine l'habileté et la chance. Le jeu peut prendre diverses formes, dont les paris sportifs et d'autres formules de jeu de hasard. (Gambling)
**Jurons :** Propos vulgaires (offensants), utilisés dans un texte écrit ou verbalement dans un fichier son ou vidéo et même dans la légende accompagnant une image. (Profanity)
**Menace :** Tout événement possible, délibéré ou accidentel, qui pourrait causer un préjudice aux employés ou aux biens. (Threat)
**Nudité :** Personne nue ou montrant ses organes génitaux. N'est pas nécessairement de nature sexuelle. (Nudity)
**Opération pyramidale :** Type d'entreprise qui vous encourage à envoyer de l'argent dans l'espoir qu'un nombre déterminé de personnes vous enverront à leur tour de l'argent. (Pyramid schemes)
**Pornographie :** Matériel à caractère explicitement sexuel conçu pour provoquer une excitation sexuelle. (Pornography)
**Pourriel :** Tout courriel non sollicité provenant de l'extérieur. La plupart des pourriels sont d'ordre publicitaire, mais certains peuvent aussi avoir un contenu de nature criminel, notamment dans le cas de la pornographie juvénile et des rackets. (Spam messages)
**Renseignement :** Bien ou ressource de l'Agence, définie comme étant un ensemble de données, de faits ou de connaissances consignés, quels qu'en soient la forme, le support ou la technologie. (Information)





**Renseignement de l'organisation :** Renseignement consigné tiré des actions, opérations, processus administratifs, fonctions et activités de l'ASFC. Un renseignement de l'organisation sert :

- de preuve du rendement de l'organisation;
- de relevé des ressources utilisées;
- d'indication du comment et du pourquoi une décision a été prise;
- de moyen de prouver que des dispositions législatives, des politiques et des normes ont été respectées;
- de pièce démontrant comment les opérations font l'objet d'un suivi échelonné sur une période;
- de souvenir rappelant le milieu de travail et les facteurs décisifs; de témoignage concernant les droits et le calcul des droits d'employés, de particuliers, de sociétés, etc.;
- de document révélant des activités qui appuient et protègent des intérêts juridiques, financiers, historiques et autres du gouvernement et du public. (Corporate information)

**Renseignements classifiés :** Information d'intérêt national qui peut être visée par une exception ou une exclusion aux termes de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels et qui, si elle est compromise, pourrait très bien nuire à l'intérêt national. (Voir également Renseignements délicats.) (Classified information)

**Renseignements délicats :** Information qui doit être adéquatement protégée en raison de son caractère confidentiel. Voir également Renseignements classifiés et Renseignements protégés. (Sensitive information)

**Renseignements protégés :** Information qui n'est pas d'intérêt national mais qui peut être visée par une exception ou une exclusion aux termes de la Loi sur l'accès à l'information or de la Loi sur la protection des renseignements personnels et qui, si elle était compromise, pourrait vraisemblablement causer un préjudice ne touchant pas l'intérêt national. (Voir également Renseignements délicats.) (Protected information)

**Renseignements transitoires :** Information nécessaire pendant une durée limitée pour terminer une mesure courante ou préparer un document ultérieur. Les renseignements transitoires comprennent les renseignements donnés dans une forme utilisée pour les communications ordinaires, les ébauches de documents contenant des commentaires et des renseignements supplémentaires destinés à des versions ultérieures, les versions des documents qui n'ont pas été communiqués à l'extérieur du bureau qui les a créés et les doubles des documents servant de référence seulement.

**Risque :** Possibilité qu'une faiblesse soit exploitée ou qu'elle entraîne un préjudice. (Risk)

**Salons de clavardage :** Tribunes électroniques permettant aux participants de discuter en ligne en temps réel, généralement par échange de messages textuels. (Chat rooms)



**Sécurité informatique :** Ensemble de précautions utilisées pour protéger la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur de l'information stockée, traitée et transmise de façon électronique. (Information technology security)
**Surveillance du contenu :** Comprend notamment l'examen du contenu et l'analyse du volume de fichiers, de courriels ou de journaux, pour déterminer s'il y a eu utilisation abusive. (Content monitoring)
**Systèmes principaux :** Bases de données, notamment les SAE, applications sur ordinateur central et applications de réseau. Ils sont réservés aux activités de l'Agence. (Primary systems)
**Systèmes secondaires :** Applications comme le courriel, Microsoft Office et Internet (qui peuvent être utilisés à certaines fins personnelles). (Secondary systems)
**Utilisation malveillante :** Toute action ou omission d'un utilisateur qui constitue une activité inacceptable, illicite ou criminelle. (Misuse)
**Valeur :** Valeur estimative, monétaire, culturelle, intellectuelle ou autre. (Value)
**Violence :** Y compris les documents dans lesquels des gestes ou des traitements insultants ou violents sur le plan physique sont décrits. (Violence)
**Virus :** Un programme qui infecte un ordinateur en s'attachant à un autre programme et qui se reproduit lorsque ce programme est exécuté. (Virus)
**Vulnérabilité :** Faiblesse liée à la sécurité et qui pourrait permettre qu'une menace se concrétise. (Vulnerability)

Canada Border Services Agency | Agence des services frontaliers du Canada



# Guidelines for the Policy on the Use of Electronic Resources

PROTECTION • SERVICE • INTEGRITY

Canada



# 1. Introduction

The Policy on the Use of Electronic Resources ensures that all CBSA employees, contractors and individuals authorized to access CBSA electronic resources use them appropriately. The policy describes approved uses of the electronic resources as well as unlawful and unacceptable uses; it defines limits of personal use, outlines employee and management responsibilities and notifies users of our monitoring practices. All individuals who access our electronic resources should familiarize themselves with this policy.

This document is based on the "Policy on the Use of Electronic Resources". It is intended to provide guidance about the responsible use of electronic resources. These guidelines outline some of your key responsibilities as a user of CBSA's electronic resources. It also provides concrete examples of how the policy applies to everyday use.

Awareness sessions will be made available to enhance your understanding, and will be in a format that can be adapted to your work schedule. We know you will continue to make appropriate use of our electronic resources because you can make a difference!

# 2. The CBSA Electronic Resources

The CBSA values of integrity, respect and professionalism should guide your use of our electronic resources. Up-to-date information systems and technology are important tools that allow CBSA employees to provide a high quality service to all our clients and stakeholders. In our daily work, we use computer systems and electronic networks to conduct CBSA business and to communicate with colleagues, clients, and the public.

Our network's capacity is under continuous pressure as increased use is made of services such as email and client service transactions, the Internet and our own intranet. Just as highways are congested in rush hour, our network is busiest during business hours. A congested network that delays transmission of client transactions has a direct and negative impact on client service. Since our network is a finite resource, it must be used responsibly in order to maintain its integrity and effectiveness.

**How** we use the network, **what** we use it for, and even **when** we use it are all things for us to consider in our day-to-day work. Please take a few moments to learn what you can do to help all of us make best use of this important corporate resource.

# 3. Your Responsibilities

The information and systems you use daily are critical to CBSA's business operations. You have a responsibility to protect information and assets.

You are the best protection available by being aware of your personal IT security responsibilities, conforming to policies, and by the diligent use of security techniques. We are all expected to use







common sense and good judgement in our work and interaction with colleagues, clients, and the public.

The following is a summary of your responsibilities. Please refer to the Policy on the Use of Electronic Resources for further details.

- Do not send sensitive information such as client and employee information using the CBSA email systems and electronic resources because they are not secure. There are potential risks that sensitive information could be read by, or misdirected to, unauthorized persons and destinations if such information is transmitted electronically without the proper controls and safeguards.
- Protect your password at all times. No one else should be permitted to use it.
- Do not engage in activities that are criminal, unlawful, or unacceptable. You can find some examples of these activities in the Policy on the Use of Electronic Resources and in the CBSA Code of Conduct.
- Report any criminal or unlawful breach of computer security, policies, and standards to your supervisor.
- Be informed of all CBSA and Government of Canada applicable policies, standards and laws.
- Contact your supervisor when in doubt about proper procedures and acceptable uses.

# 4. Best Practices

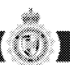
You are responsible and accountable for everything you do while using the electronic resources. There are basic steps that you can follow to keep CBSA's information and assets secure, including your workstation, the photocopier, the facsimile machine and the printer.

Take a few moments to view the following presentation, Information Technology (IT) Security Basics.

# 5. Need-to-know Principle

Access to CBSA systems and information is limited to those with a "**need-to-know**" that restricts the information that can be accessed. This means it is limited to users with the appropriate screening level, and that users only have access to information and systems that are required to fulfill their job. For example, although two people may have the same screening level, such as a Secret security clearance, but their official work duties are different, they will not be authorized to access the same information or systems. Also, they must not share the information that they have accessed.

As a user you must not access CBSA information about yourself, your colleagues, your relatives, your friends and acquaintances or non work related individuals under any circumstances, except where access to that information is directly related to an authorized program or activity required to perform your job.



# 6. Monitoring

CBSA monitoring occurs mainly for operational reasons to determine whether the resources/networks are operating efficiently, to isolate and resolve problems, and to determine if utilization complies with CBSA policies and legislation. Refer to the Policy on the Use of Electronic Resources for more details.

When you login to your system, you must press CTRL + ALT+ DELETE.
A banner then appears and reads as follows:

The use of Canada Revenue Agency/Canada Border Services Agency networks, systems, computers and/or databases is subject to monitoring by CRA or CBSA Information Technology personnel, and an audit log may be implemented and reviewed by CRA or CBSA. Anyone using this information technology at CRA or CBSA implicitly consents to such monitoring. Any unauthorized use by employees or any other person may result in disciplinary action and/or criminal prosecution.

The purpose of the banner is to inform you that the electronic resources, network and computer systems are subject to monitoring.

Next time you login to your system, take a moment to read the banner.

# 7. User ID and Password

CBSA provides you with a unique user ID to access electronic resources via your workstation or laptop.

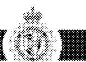
Some users have specialized accounts that provide additional privileges, such as IT operational personnel who set up your workstation and install authorized software. The use of these accounts is only to perform activities related to that function. Otherwise, they must use their personal User ID for all other work, such as reading their e-mail.

### *Passwords*

To gain access to the network and electronic resources, you must enter your user ID and a password.

Upon your first logon to the system, a default password will be provided to you. The system will prompt you to enter a new, unique password. Here are some guidelines on how to create a strong and secure password.

- Your password should be 8 characters in length
- It should contain at least one uppercase letter (i.e. A)
- It should contain at least one lowercase letter (i.e., b)



- It should include one number
- It should include one special character such as & * % $ # @ !

Do not use anything that can be associated with you or words from a dictionary, no matter what the language. Create a phrase that can be easily remembered and use the first characters to create your password. Transpose letters, such as E for a 3, the number 1 for the letter "I" or "L".

Here are 2 examples of strong passwords:

Three blind mice, see how they run - becomes: 3bM!Chtr#
I wish today was Friday - becomes 1w2D!wf$

To make sure that access to your system is always secure, you will be prompted every 90 days to change your password and create a new unique password. You must remember that there exists a password history that will not allow you to use the same passwords you have recently used.

Finally, remember that you must **never** share your password. Your password is the only way you can identify yourself to systems.

For further details regarding passwords, refer to the "Password Tips" document from the IT Security Intranet.

# 8. Protecting Your Information

## Where do I save information?

Sensitive information must be saved on your personal network H: drive or an authorized group share. Backups of information residing on the H: drive are executed daily so that your data can be recovered in the event of a disaster.

Never store sensitive information on a local drive such as C:, D:, or E:

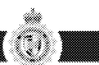
## Protecting my system access

Do not leave your workstation unattended where an unauthorized person could gain access to your system.

When you walk away for any extended period of time (lunch, meetings, breaks), always lock your workstation. Press CTRL + ALT + DEL and select the "Lock your Computer" option.

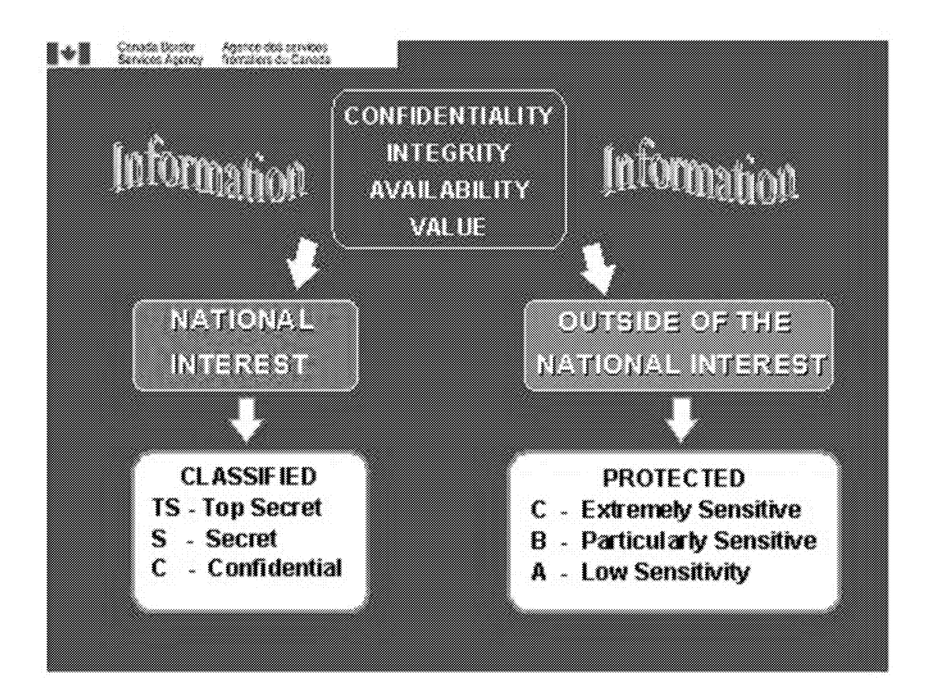
Ensure you shut down your system at the end of each day. This will allow system updates to be applied when you reboot your workstation.

# 9. What is Sensitive Information?



The Government of Canada categorizes information as "Unclassified", "Protected" and "Classified". Most of the sensitive information you deal with is considered Protected "A" and/or Protected "B".

The main difference between Protected and Classified information is the type of injury that could occur in the event of unauthorized disclosure of the sensitive information. The figure below summarizes the levels of Protected and Classified information and if it impacts the "National Interest" of Canada.




Confidentiality, Integrity, Availability, Value
- National Interest
  - Classified
    - TS - Top Secret
    - S - Secret
    - C - Confidential
- Outside of National Interest
  - Protected
    - C - Extremely Sensitive
    - B - Particularly Sensitive
    - A - Low Sensitivity

# 9. What is Sensitive Information? (cont'd)

## Protected A

Unauthorized release could cause injury to an individual, organization or government.



Loss of Privacy
Embarrassment

Examples of Protected "A" information can include home addresses, telephone numbers, date of birth or salaries. You should note that a combination of some information may result in Protected "B" information.

## Protected B

Unauthorized release could cause serious injury to an individual, organization or government.

Prejudicial treatment
Loss of reputation or competitive edge

Examples of Protected "B" information can include competitive position of a third party, criminal information on an individual, performance evaluations, financial, religious or political beliefs or information received "in confidence" from other government organizations.

## Protected C

Unauthorized release could cause extremely serious injury to an individual, organization or government.

Significant financial loss
Loss of life

Examples of Protected "C" information can include Information that could cause the bankruptcy of an individual or company, testimony against another individual or Informant information that cause result in physical harm or death to an individual.

## Classified Information

The category of classified information recognizes that the information "in the national interest" is vital to the security of the nation - its defence, or the maintenance of social, political and economic stability in Canada.

Examples of Classified information can include documents such as those concerned with Federal-provincial relations, Cabinet papers, information involving security, international affairs, advice and recommendations and intelligence or security.

To obtain further details regarding information sensitivity, please access the Procedures for Identification, Categorization and Marking of Information Assets available from Corporate Security.

# 10. E-mail



E-mail is intended for corporate use. Do not distribute chain letters, jokes or games, executable file attachments or large file attachments (for example, pictures). If a large amount of these types of files or documents are sent via the e-mail system, it can overload the services and "crash" the system. It may take significant effort to restore the email service.

You need to be conscientious when sending e-mail. E-mail remains stored on CBSA systems, even after the originator or recipient has deleted the message. Also, once e-mail is sent outside the control of CBSA systems, such as via the Internet, it can be intercepted or altered, unless encrypted. An email message sent outside of the Agency is like a postcard: anyone can read it therefore as a user you should not have an expectation of privacy.

Here are a few tips when sending or receiving e-mail:

- Think, write, read, and edit before sending e-mail.
- Keep messages brief and concise.
- Before sending, check who are in the group distribution lists.
- Make sure lists are updated regularly.
- If you are part of a distribution list, do not select "Reply to All" unless necessary.
- Be sure that each person on a distribution list has a "Need-to-know" of the e-mail message content or attached documents.
- Do not open attachments unless you first know whom it is truly from.
- Do not respond to unsolicited e-mails, such as messages received from unknown senders.
- If the message contains sensitive information, there may be a need to encrypt it. (see below for details regarding encryption).

You should be aware that all files, including internal and external e-mail messages are logged for business purposes. CBSA also logs Internet sites individuals have visited using CBSA equipment.

# 11. Email Delegation

You must never share your password to allow someone to access your email account. Good news! You can securely share your account by delegating your e-mail access.

MS (Microsoft) Outlook allows you to authorize someone to read, write and/or modify messages from your account during your absence.

The following steps will detail how you can turn on the delegation option and choose the permissions you want to delegate.

- From the MS Outlook Standard Toolbar, click on Tools, Options.
- Click on the "Delegates" tab.
- Click on "Add".
- Select a User Name from the Global Address List, click on "Add" and click on OK.
- The name will appear in the right hand box "Add Users".
- A new box will open.
- Click on the down arrow for the "Inbox" option to delegate permissions.
- Select one of the options. (Reviewer, Author or Editor).
- Click OK.



- Click on "Apply" and then "OK" to complete the delegation process.

Remember to turn off the delegation of your email account once you return to the office.

If leave is unanticipated and you are unable to setup delegation authority prior to your leave, a request can be submitted to the Information Security's Network Monitoring group to perform this operation on your behalf, including any delegate permissions and adding or maintaining an Out of Office reply. If you are unable to provide direct authorization for any reason, your Director may also submit a request in your absence. For more information regarding this topic, you can send a message to the Information Security mailbox: information_security-securite_de_linformation@cbsa-asfc.gc.ca.

# 12. Information Searches

As a user of CBSA systems, you have a reasonable expectation of privacy. There may be circumstances when you are absent from the office for an extended period of time and there is a business requirement to access some of your files.

Before an electronic information search can take place, the following must be considered:

- There is no other means to obtain the information.
- The search for information is to support business requirements.
- All requests require Director-level approval if you are unable to provide authorization.

Corporate Information Security is responsible for searching and accessing files from a user's electronic mailbox, H: Drive, and/or workstation, based on business requirements. If an information search is approved, Information Security's Network Monitoring group will review and extract the required files/folders/emails and provide a copy of the requested information to your Director. Prior to releasing any information, Network Monitoring must review and remove any private information from the request. All unrelated information is not to be divulged.

Management must notify you that a retrieval of information has taken place during your absence.

Your best bet...

When leave is anticipated, you should provide all required documentation to your manager **before** you leave or make your documents available during your absence by placing them on a designated group share. This ensures your office can continue to function without any unnecessary delays.

For more information regarding this topic, you can send a message to the Information Security mailbox: information_security-securite_de_linformation@cbsa-asfc.gc.ca.

# 13. Encryption

Appropriate safeguards must be implemented to protect sensitive information when in electronic form (both in storage and in transit). A Public Key Infrastructure (PKI) provides a set of tools





that will allow you to protect sensitive information. PKI provides two mechanisms known as encryption and digital signature.

Encryption converts information of an original message by means of a mathematical code in such a way that the content is unreadable by unauthorized users. This means that only the intended authorized user, by using a secret key, can read the content.

Encryption provides data confidentiality, a protection against unauthorized disclosure. It also offers access control: it ensures that only authorized users are permitted to access the message and attachments.

A digital signature is like a paper signature, but it is electronic. A digital signature provides verification to an e-mail recipient that the message came from the person who sent it (authentication). It also confirms that the original content of the message has not been altered (integrity). Also, the sender cannot deny that the message was sent (non-repudiation).

CBSA uses PKI to enable individuals to securely send e-mail to other organizations and enable connectivity with authorized users for secure information sharing. It also will allow users to utilize Secure Remote Access services (gaining access to the corporate network and e-mail system offsite, such as at home or during travel status).

Encryption, password-protected media and software can also help users keep information secure. Sensitive information and data stored on various types of media, particularly portable and removable media, such as USB memory sticks, laptops and hard drives must be protected. For example, laptops provided by CBSA are configured with encryption software to protect the information that resides on the hard drive.

If you think you require encryption and/or digital signature services to protect electronic information, please speak to your supervisor.

## 14. Social Engineering

Social engineering is the practice of obtaining privileged information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against policies.

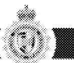
Social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes.

Here are a few tips to avoid the traps of a social engineer:

- Verify the source of a call or request by Internet for information. Ask for a number to call back or initiate the Internet session yourself (i.e. email message received from your Bank).
- Never share or reveal your password
- An Information Technology technician does not need your password to update or fix your system. They will not ask you for your password or credentials over the phone.
- Trust your intuition - Your "gut feeling" usually triggers a sense that something is off or not quite right.







- If in doubt, check the source and report it.

# 15. Identity Theft

Identity theft is the deliberate impersonation of another person's identity, usually to gain access to their finances, make purchases or frame them for a crime. Identity theft occurs when someone steals your personal information such as birth date, Social Insurance Number, passport, address, name, and bank account information, usually without your knowledge. Less commonly, it is to enable illegal immigration, terrorism, espionage, or changing identity permanently.

For further details on Identity Theft and how to prevent it, you can access the following presentation from the IT Security Intranet site: Protect your Identity - Prevent Identity Theft.

# 16. Reporting Security Incidents

A security incident is any activity involving, for example:

- Theft, loss or destruction of revenue, money, seized, held or other assets belonging to or in the care of CBSA.
- Abuse, threats, stalking and assaults against employees.
- Suspected or actual compromise of protected and/or classified information.
- Malicious codes and virus alerts/attacks against CBSA communication or computer systems or other circumstances leading to system degradation (Do not forward files or email if you think you have a virus, call the IT help desk).
- Loss, theft or misuse of identification/access cards, building passes, authorization cards and keys.
- Incidents impacting on the physical security of a CBSA building or facility leading to a closure or evacuation such as a power outage, fire, vandalism, flood or weather hazard.
- Incidents suspected of constituting unacceptable, illegal or criminal offences.
- Incidents that have an impact on government operations or that could require revisions to operational standards or technical documentation.

To find out how to report a security incident, you can access the Corporate Security Intranet site for details on Reporting Security Incidents.

This document was developed by IT Security of the Innovation, Science and Technology Branch in collaboration with Corporate Security and Internal Affairs of the Comptrollership Branch.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Lignes directrices concernant la Politique sur l'utilisation des ressources électroniques

PROTECTION • SERVICE • INTÉGRITÉ

Canada



# 1. Introduction

La Politique sur l'utilisation des ressources électroniques a pour but de veiller à ce que tous les employés de l'ASFC, tous les entrepreneurs qui font affaire avec l'ASFC et toutes les autres personnes qui sont autorisés à accéder aux ressources électroniques de l'ASFC les utilisent comme il se doit. La politique décrit les activités pour lesquelles l'utilisation des ressources électroniques est approuvée ainsi que les activités illicites et inacceptables qui sont à proscrire; elle définit les conditions d'utilisation personnelle limitée, elle trace les grandes lignes concernant les responsabilités des employés et de la direction et informe les utilisateurs au sujet des types de surveillance exercée par l'ASFC. Toute personne qui a accès aux ressources électroniques de l'ASFC devrait se familiariser avec cette politique.

Le présent document est basé sur la « Politique sur l'utilisation des ressources électroniques ». Il vise à fournir des consignes claires sur l'utilisation responsable des ressources électroniques, et il décrit quelques-unes des principales responsabilités des utilisateurs des ressources électroniques de l'ASFC. De plus, on y trouve aussi des exemples concrets de la façon dont la politique s'applique à l'utilisation quotidienne des ressources.

Des séances de sensibilisation seront offertes, dans un format qui pourra être adapté à votre horaire de travail, pour vous aider à mieux comprendre la Politique. Nous savons que vous continuerez à utiliser nos ressources électroniques de façon appropriée, et vous pourrez ainsi faire toute une différence!

# 2. Les ressources électroniques de l'ASFC

Les valeurs d'intégrité, de respect et de professionnalisme de l'ASFC devraient guider l'utilisation que vous faites des ressources électroniques. Les technologies de l'information et les systèmes d'information à jour constituent des outils importants qui permettent aux employés de l'ASFC de fournir un service de grande qualité à tous les clients et intervenants. Dans le cadre de nos activités quotidiennes, nous utilisons des systèmes informatiques et des réseaux électroniques pour exécuter les travaux de l'ASFC et communiquer avec nos collègues, clients et avec le public.

La capacité de notre réseau fait l'objet d'une pression continue à mesure que les services, tels le courriel et les transactions de service aux clients ainsi que l'Internet et notre propre intranet, sont des plus en plus utilisés. Tout comme le trafic sur le réseau routier qui devient dense aux heures de pointe, le trafic sur notre réseau est le plus intense pendant les heures de travail. Un réseau encombré qui ralentit la transmission des transactions avec les clients a une incidence directe et négative sur le service offert aux clients. Étant donné que notre réseau est une ressource limitée, il doit être utilisé de façon responsable pour que son intégrité et son efficacité puissent être conservées.

**Comment** nous utilisons le réseau, à **quelle fin** nous l'utilisons et **quand** nous l'utilisons sont toutes des questions que nous devons considérer dans le cadre de notre travail quotidien.



Veuillez prendre quelques instants pour découvrir ce que vous pouvez faire afin que nous fassions ensemble le meilleur usage possible de cette importante ressource de l'Agence.

# 3. Vos responsabilités

L'information et les systèmes que vous utilisez tous les jours sont essentiels aux activités opérationnelles de l'ASFC. Il vous incombe donc de protéger l'information et les biens de l'Agence.

Vous êtes la meilleure mesure de protection qui soit disponible, si vous êtes au courant de vos responsabilités en matière de sécurité des TI et que vous les respectez, si vous vous conformez aux politiques et si vous appliquez avec diligence les techniques de sécurité. Nous sommes tous appelés à faire preuve de bon sens et de jugement dans le cadre de notre travail et de nos relations avec nos collègues, nos clients et le public.

Voici un résumé de vos responsabilités. Veuillez consulter la Politique sur l'utilisation des ressources électroniques pour obtenir des détails supplémentaires.

- N'envoyez pas de renseignements de nature sensible, p. ex. des renseignements sur les clients et les employés, au moyen des systèmes de messagerie et des ressources électroniques de l'ASFC, parce qu'ils ne sont pas protégés. Il y a des risques que ces renseignements soient lus par des personnes ou des destinataires non autorisés ou qu'ils leur soient envoyés par erreur, si ces renseignements sont transmis électroniquement sans l'utilisation de contrôles et de mesures de protection appropriés.
- Protégez votre mot de passe en tout temps. Aucune autre personne ne devrait avoir le droit de l'utiliser.
- Ne vous livrez à aucune activité criminelle, illicite ou inacceptable. Vous pouvez trouver des exemples de telles activités dans la Politique sur l'utilisation des ressources électroniques et dans le Code de conduite de l'ASFC.
- Signalez à votre superviseur toute violation (activité criminelle ou illicite) des politiques et des normes de sécurité informatique.
- Soyez au courant de toutes les politiques, les normes et les lois applicables de l'ASFC et du gouvernement du Canada.
- Communiquez avec votre superviseur en cas de doute sur les procédures appropriées et l'utilisation acceptable.

# 4. Pratiques exemplaires

Vous êtes responsable de toutes les activités que vous réalisez en utilisant les ressources électroniques, et vous êtes tenu de rendre compte de toutes ces activités. Il existe des étapes élémentaires que vous pouvez suivre pour protéger l'information et les biens de l'ASFC. Elles s'appliquent notamment à votre poste de travail, à la photocopieuse, au télécopieur et à l'imprimante.

Prenez quelques instants pour visualiser la présentation suivante : Notions de base de la sécurité des technologies de l'information.



## 5. Principe du besoin de connaître

L'accès à l'information et aux systèmes de l'ASFC est limité aux seuls utilisateurs qui ont **besoin de connaître** ou d'utiliser ces derniers, ce qui limite l'information à laquelle on peut accéder. Cela veut dire que l'accès est accordé seulement aux utilisateurs ayant la cote de sécurité appropriée, et que les utilisateurs ont seulement accès à l'information et aux systèmes dont ils ont besoin pour s'acquitter de leurs fonctions. Supposons que deux personnes ont la même cote de sécurité, p. ex. la cote Secret, elles ne seront pas autorisées à accéder à la même information et aux mêmes systèmes si leurs fonctions officielles diffèrent. De plus, elles ne doivent pas partager l'information à laquelle elles ont eu accès.

En tant qu'utilisateur, vous ne devez en aucun cas accéder à l'information que l'ASFC conserve sur vous, vos collègues, vos parents, vos amis, vos connaissances et sur toute autre personne n'ayant aucun rapport avec votre travail, sauf lorsque l'accès à cette information est directement relié à un programme ou à une activité autorisés requis dans l'exécution de vos fonctions.

## 6. Surveillance

L'ASFC exerce une surveillance principalement pour des raisons opérationnelles afin de déterminer si les ressources/réseaux fonctionnent de façon efficace, d'identifier et de résoudre les problèmes et de déterminer si l'utilisation est conforme aux politiques et aux lois de l'ASFC. Consultez la Politique sur l'utilisation des ressources électroniques pour obtenir des détails supplémentaires.

Lorsque vous voulez ouvrir une session dans le système, vous devez appuyer sur les touches CTRL + ALT + DELETE. L'énoncé suivant s'affiche :

- L'utilisation des réseaux, des systèmes, des ordinateurs et des bases de données de l'Agence du revenu du Canada/Agence des services frontaliers du Canada est contrôlée par les employés de la technologie de l'information de l'ARC ou l'ASFC, et un registre de vérification peut être établi et examiné par l'ARC ou l'ASFC. Quiconque a recours à cette technologie à l'ARC ou à l'ASFC consent implicitement à faire l'objet d'un tel contrôle. Toute utilisation non autorisée par des employés ou par toute personne peut entraîner des mesures disciplinaires ou aussi des poursuites criminelles.
- Cet énoncé a comme but de vous informer de la surveillance dont font l'objet les ressources électroniques, le réseau et les systèmes informatiques.
- La prochaine fois que vous ouvrirez une session dans le système, prenez le temps de lire cet énoncé.

## 7. Nom d'utilisateur et mot de passe

L'ASFC vous attribue un nom d'utilisateur unique pour accéder aux ressources électroniques à partir de votre poste de travail ou de votre ordinateur portatif.

Certains utilisateurs ont des comptes spécialisés grâce auxquels ils ont des privilèges supplémentaires, p. ex. le personnel opérationnel des TI qui configure votre poste de travail et



installe les logiciels autorisés. L'utilisation de ces comptes est réservée aux activités reliées à ces fonctions. Autrement, ils doivent utiliser leur nom d'utilisateur personnel pour tout autre travail, comme c'est le cas pour lire leurs messages de courriel.

### Mots de passe

Pour accéder au réseau et aux ressources électroniques, vous devez entrer votre nom d'utilisateur et votre mot de passe.

Pour que vous puissiez ouvrir une première session dans le système, un mot de passe par défaut vous sera fourni. Le système vous demandera d'entrer un nouveau mot de passe unique. Voici quelques règles à suivre pour créer un mot de passe sûr/difficile à deviner :

- Votre mot de passe doit comporter huit caractères.
- Il devrait contenir au moins une lettre majuscule (p. ex. A).
- Il devrait contenir au moins une lettre minuscule (p. ex. b).
- Il devrait contenir un chiffre.
- Il devrait contenir un caractère spécial, p. ex. & * % $ # @ !

N'utilisez aucun mot qui puisse vous être associé ou qui provienne du dictionnaire, peu importe la langue. Composez une phrase qui soit facile à retenir et utilisez les premières lettres pour créer votre mot de passe. Remplacez des lettres, p. ex. remplacez un « E » par un « 3 », ou encore, remplacez les lettres « I » ou « L » par le numéro « 1 ».

Voici deux exemples de mots de passe sûrs :

« Trois souris aveugles, regardez comme elles courent » pourrait devenir « 3sA!rcec# »
« Comme j'aimerais que ce soit lundi! » pourrait devenir « Cja!qs1$ ».

Afin de s'assurer que l'accès à votre système demeure toujours sécurisé, vous serez invité à tous les 90 jours de changer votre mot de passe. Vous devez créer un nouveau mot de passe tout à fait unique car il existe un historique qui ne vous permettra pas d'en utiliser un que vous avez récemment créé.

Finalement, souvenez-vous qu'il ne faut **jamais** donner votre mot de passe. Votre mot de passe est le seul moyen pour les systèmes de valider votre identité.

Pour obtenir d'autres détails concernant les mots de passe, consultez le document intitulé « Astuces concernant les mots de passe » à partir du site Web intranet de la section de la sécurité informatique.

## 8. Protection de vos renseignements

### Où dois-je enregistrer les renseignements?



Les renseignements de nature sensible (nature délicate) doivent être enregistrés sur votre lecteur réseau personnel (lecteur H:) ou sur un lecteur partagé de groupe. Des copies de sauvegarde des renseignements se trouvant dans le lecteur H: sont effectuées tous les jours, de sorte que les données peuvent être récupérées en cas de désastre.

N'enregistrez jamais des renseignements de nature sensible dans un lecteur local, p. ex. les lecteurs C:, D: ou E:.

### Protection de l'accès au système

Ne laissez pas votre poste de travail sans surveillance, car une personne non autorisée pourrait accéder à votre système.

Lorsque vous vous éloignez de votre poste pendant une période prolongée (dîner, réunion, pause), verrouillez toujours votre poste de travail. Appuyez sur les touches CTRL + ALT + DEL, et sélectionnez l'option « Verrouiller le poste ».

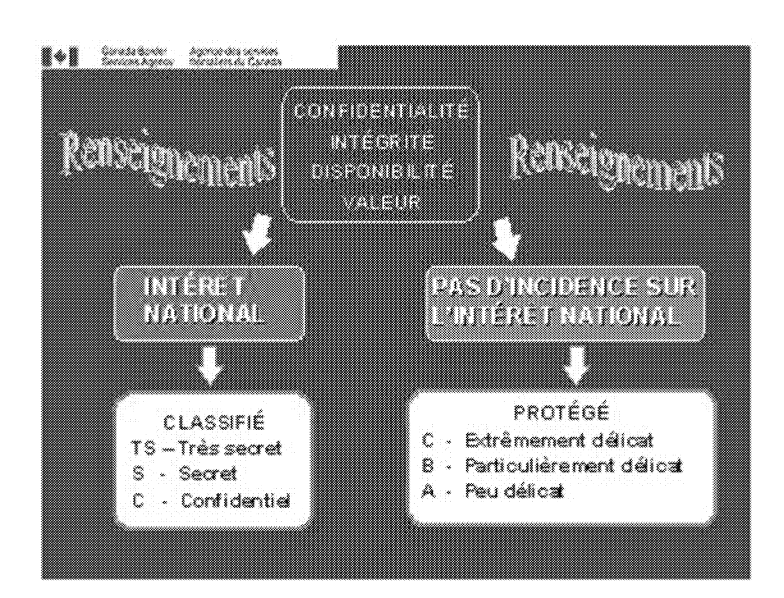
Assurez-vous de fermer votre système à la fin de la journée; les mises à jour du système pourront alors être effectuées lors du redémarrage.

## 9. En quoi consistent les renseignements de nature sensible?

Le gouvernement du Canada classe les renseignements selon les catégories « Non classifié », « Protégé » et « Classifié ». La plupart des renseignements de nature sensible (souvent désigné sous le terme « nature délicate ») auxquels vous avez affaire sont classés « Protégé A » et/ou « Protégé B ».

Le type de préjudice découlant de la divulgation non autorisée des renseignements de nature sensible constitue la principale différence entre les renseignements portant la mention « Protégé » et ceux portant la mention « Classifié ». La figure suivante résume les différents niveaux « Protégé » et « Classifié » ainsi que l'incidence de la divulgation de renseignements de ces niveaux sur l'intérêt national du Canada.






ConfidentIalité, Intégrité, Disponibilité, Valeur

- intérêt national
  - Classifié
    - TS - Très secret
    - S - Secret
    - C - Confidentiel
- Pas d'incidence sur l'intérêt national
  - Protégé
    - C - Extrêmement délicat
    - B - Particulièrement délicat
    - A - Peu délicat

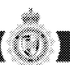
# 9. En quoi consistent les renseignements de nature sensible (suite)

## Protégé A

La diffusion non autorisée pourrait causer des préjudices à une personne, à une organisation ou au gouvernement.

- Atteinte à la vie privée
- Embarras

Voici quelques exemples de renseignements « Protégé A » : les adresses et numéros de téléphone personnels, les dates de naissance et les salaires. Prenez note que certains renseignements mis ensemble peuvent être désignés « Protégé B ».



## Protégé B

La diffusion non autorisée pourrait causer des préjudices graves à une personne, à une organisation ou au gouvernement.

- Traitement préjudiciable
- Perte de réputation ou d'avantage concurrentiel

Voici quelques exemples de renseignements « Protégé B » : position concurrentielle d'une tierce partie, renseignements personnels (dossier criminel, finances, religion, allégeance politique), évaluations de rendement ou renseignements reçus à titre confidentiel d'autres organisations du gouvernement.

## Protégé C

Une divulgation non autorisée pourrait causer un préjudice extrêmement grave à un particulier, à un organisme ou au gouvernement.

- Perte de sommes d'argent considérables
- Perte de vie

Voici quelques exemples de renseignements « Protégé C » : de l'information qui pourrait causer la faillite d'une personne ou d'une organisation, témoignage contre une autre personne ou de l'information d'un informateur qui pourrait causer des dommages corporels à une personne ou la mort d'une personne.

## Renseignements classifiés

La catégorie « classifié » existe parce qu'il y a des renseignements qui ont une incidence sur l'intérêt national et qui ont une importance vitale pour la sécurité de la nation - nommément la défense et le maintien de la stabilité sociale, politique et économique du Canada.

Voici quelques exemples de documents classifiés : les documents portant sur les relations fédérales-provinciales, les documents du Cabinet, les documents relatifs à la sécurité, aux affaires internationales, aux conseils et aux recommandations et au renseignement.

Pour obtenir d'autres détails concernant la nature sensible des renseignements, veuillez consulter les Procédures d'identification, de catégorisation et de marquage des ressources d'information, qui sont accessibles sur le site de la sécurité de l'Agence.

# 10. Courriel

Le courriel doit être utilisé à des fins opérationnelles. Ne transférez pas des lettres en chaîne, des blagues ou des jeux, des fichiers exécutables ou des gros fichiers comme pièces jointes (par exemple, des images). Si un grand nombre de ces types de messages sont envoyés au moyen du système de messagerie, ce dernier peut tomber en panne sous le fardeau d'une telle surcharge. Il se pourrait qu'un effort important soit requis pour remettre le système en service.

Vous devez faire preuve de jugement lorsque vous envoyez des messages. En effet, ces derniers demeurent stockés dans les systèmes de l'ASFC, même après que l'expéditeur ou le destinataire les ait supprimés. De plus, une fois qu'un message se retrouve à l'extérieur du contrôle exercé par les systèmes de l'ASFC (sur Internet), il peut être intercepté ou altéré, à moins qu'il ne soit chiffré. Un message envoyé à l'extérieur de l'Agence est comme une carte postale; n'importe qui peut le lire. Par conséquent, en tant qu'utilisateur, vous ne devriez pas vous attendre à ce que les renseignements transmis de cette façon ne soient protégés.

Voici quelques astuces que vous pouvez appliquer lorsque vous envoyez ou recevez des messages :

- Réfléchissez, puis rédigez, relisez et modifiez votre message avant de l'envoyer.
- Rédigez des messages courts et concis.
- Avant d'envoyer un message, vérifiez qui fait partie de la liste de distribution.
- Mettez les listes à jour régulièrement.
- Si vous faites partie d'une liste de distribution, ne sélectionnez pas « Répondre à tous », sauf lorsque c'est vraiment nécessaire.
- Assurez-vous que chaque personne dans la liste de distribution a besoin de connaître le contenu du message ou des pièces jointes.
- N'ouvrez pas les pièces jointes, sauf si vous savez qui les envoie réellement.
- Ne répondez pas aux messages non sollicités, p. ex. des messages provenant d'expéditeurs inconnus.
- Si le message contient des renseignements de nature sensible, il faudrait peut-être qu'il soit chiffré (voyez ci-dessous les détails concernant le chiffrement).

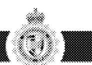
Vous devriez savoir que tous les fichiers, y compris les messages internes et externes, sont enregistrés à des fins opérationnelles. L'ASFC conserve aussi un registre de tous les sites Internet visités en utilisant de l'équipement lui appartenant.

# 11. Délégation de l'accès à la boîte aux lettres électronique

Vous ne devez jamais donner votre mot de passe pour que quelqu'un puisse accéder à votre compte de courriel. Bonnes nouvelles! Vous pouvez permettre à quelqu'un d'autre d'accéder à votre compte de façon sécuritaire en déléguant l'accès à votre boîte aux lettres.

MS (Microsoft) Outlook vous permet d'autoriser quelqu'un d'autre à lire, à rédiger et/ou à modifier des messages dans votre compte pendant votre absence.

Les étapes ci-dessous décrivent en détail comment activer l'option de délégation et choisir les permissions que vous voulez déléguer.



- Dans la barre d'outils standard de MS Outlook, sélectionnez « Options » dans le menu Outils.
- Cliquez sur l'onglet « Délégués ».
- Cliquez sur le bouton « Ajouter ».
- Sélectionnez un nom d'utilisateur dans la liste d'adresses globale, puis cliquez sur « Ajouter ».
- Le nom apparaîtra dans la boîte « Ajouter des utilisateurs ». Cliquez sur « OK ».
- Une nouvelle boîte s'ouvrira.
- Cliquez sur la liste déroulante du champ « Boîte de réception » pour choisir les permissions à déléguer.
- Sélectionnez une des options dans la liste (Relecteur, Auteur, Rédacteur).
- Cliquez sur « OK ».
- Cliquez sur « Appliquer », puis sur « OK » pour terminer le processus de délégation.

Veuillez-vous rappelez de désactiver la délégation de l'accès à votre compte de courriel lors de votre retour au bureau.

Si votre absence n'était pas prévue et que vous ne pouvez pas configurer la délégation de l'accès avant votre départ, une demande peut être présentée au groupe responsable de la surveillance du réseau, faisant partie de la Sécurité de l'information, pour qu'ils s'occupent, à votre place, de déléguer l'accès, y compris les permissions, et d'ajouter ou de tenir à jour votre message d'absence du bureau. Si, pour une raison quelconque, vous ne pouvez pas fournir une autorisation de demande directement, votre directeur peut le faire à votre place (en votre absence). Pour obtenir plus de renseignements à ce sujet, vous pouvez envoyer un message à la boîte aux lettres de la Sécurité de l'information : information_security-securite_de_linformation@cbsa-asfc.gc.ca.

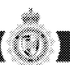
# 12. Recherches de renseignements

En tant qu'utilisateur des systèmes de l'ASFC, vous avez certaines attentes raisonnables en ce qui concerne la protection de la vie privée. Pendant que vous êtes absent du bureau pour une période prolongée, il est possible qu'il soit nécessaire, pour des raisons opérationnelles, d'accéder à certains de vos fichiers.

Avant qu'une recherche de renseignements électronique ne soit effectuée, il faut s'assurer que les conditions ci-dessous sont respectées.

- Il n'y a aucun autre moyen d'obtenir les renseignements.
- La recherche de renseignements est effectuée pour répondre à des besoins opérationnels.
- Toutes les demandes requièrent l'approbation d'un directeur si l'employé n'est pas en mesure de fournir l'autorisation.

La sécurité de l'information de l'Agence est responsable de la recherche de fichiers dans la boîte aux lettres électronique, le lecteur H: et/ou le poste de travail des utilisateurs et de l'accès aux fichiers en question, selon les besoins opérationnels. Si une recherche de renseignements est approuvée, le groupe responsable de la surveillance du réseau, faisant partie de la Sécurité de l'information, examinera et extraira les fichiers/dossiers/messages de courriel requis et fournira une copie des renseignements demandés à votre directeur. Avant de diffuser les renseignements, quels qu'ils soient, le groupe responsable de la surveillance du réseau doit



examiner et retirer tout renseignement considéré comme confidentiel. Tous les renseignements non pertinents ne doivent pas être divulgués.

Par ailleurs, la direction doit vous aviser que des renseignements ont été récupérés dans votre boîte aux lettres électronique, lecteur H: et/ou poste de travail, pendant votre absence.

Ce qu'il y a de mieux à faire...

Lorsque votre absence est prévue, vous devriez fournir tous les documents requis à votre gestionnaire **avant** de partir ou encore, les rendre accessibles pendant votre absence en les plaçant dans un lecteur partagé de groupe désigné. Cela permet d'assurer la continuité des opérations dans votre bureau, en évitant les délais inutiles.

Pour obtenir plus de renseignements à ce sujet, vous pouvez envoyer un message à la boîte aux lettres de la Sécurité de l'information : information_security-securite_de_linformation@cbsa-asfc.gc.ca.

# 13. Chiffrement

Des mesures de protection appropriées doivent être mises en œuvre pour protéger les renseignements de nature sensible lorsque ceux-ci sont en format électronique (qu'ils soient stockés ou en cours de transmission). L'infrastructure à clés publiques (ICP) vous fournit un ensemble d'outils permettant de protéger ce type de renseignements. L'ICP offre deux mécanismes : le chiffrement et la signature numérique.

Le chiffrement convertit les renseignements contenus dans le message d'origine au moyen d'un code mathématique de telle façon qu'ils deviennent illisibles par les utilisateurs non autorisés. En d'autres mots, seul l'utilisateur autorisé visé par le message peut en lire le contenu à l'aide d'une clé secrète.

Le chiffrement permet d'assurer la confidentialité des données, et il offre une protection contre la divulgation non autorisée. Il permet aussi de contrôler l'accès : seuls les utilisateurs autorisés pourront accéder au message et à ses pièces jointes.

Une signature numérique ressemble à une signature normale sur papier, mais elle est électronique. Elle permet au destinataire de vérifier que le message provient bel et bien de l'expéditeur mentionné (authentification). Elle confirme aussi que le contenu original du message n'a pas été altéré (intégrité). Enfin, l'expéditeur ne peut pas nier qu'il a envoyé le message (non-répudiation).

L'ASFC utilise l'ICP pour permettre l'envoi de messages électroniques à d'autres organisations et la connectivité entre utilisateurs autorisés afin de partager des renseignements de façon protégée. Grâce à l'ICP, les utilisateurs pourront aussi utiliser les services d'accès à distance protégé (obtenir l'accès au réseau et au système de messagerie de l'Agence à l'extérieur du bureau, p. ex. de la maison ou d'ailleurs si les utilisateurs sont en voyage).



Le chiffrement, les logiciels et les supports utilisant un mot de passe peuvent aussi aider les utilisateurs à protéger les renseignements. Les renseignements et les données de nature sensible enregistrés sur différents types de supports, particulièrement sur des supports portatifs et amovibles, comme les clés USB, les ordinateurs portables et les disques durs, doivent être protégés. Par exemple, les ordinateurs portatifs fournis par l'ASFC comportent un logiciel de chiffrement afin de protéger les renseignements enregistrés sur le disque dur.

Si vous pensez avoir besoin de services de chiffrement et/ou d'une signature numérique afin de protéger les renseignements électroniques, veuillez communiquer avec votre superviseur.

# 14. Ingénierie sociale

L'ingénierie sociale est la pratique consistant à obtenir des renseignements privilégiés en manipulant des utilisateurs légitimes. L'ingénieur social utilisera habituellement le téléphone ou Internet pour tromper une personne et la faire divulguer des renseignements de nature sensible ou la convaincre de faire quelque chose allant à l'encontre des politiques.

Les ingénieurs sociaux exploitent la tendance naturelle des gens à faire confiance, plutôt que d'exploiter les lacunes de sécurité informatique.

Voici quelques astuces pour éviter les pièges tendus par un ingénieur social :

- Vérifiez d'où provient l'appel ou la demande de renseignements (Internet). Demandez un numéro de téléphone pour rappeler ou amorcez la session Internet vous-même (p. ex. dans le cas d'un message provenant de votre banque).
- Ne donnez/divulguez jamais votre mot de passe.
- Un technicien de la TI n'a pas besoin de votre mot de passe pour mettre à jour ou réparer votre système. Il ne vous demandera pas de lui donner votre mot de passe ou des renseignements d'identité par téléphone.
- Faites-vous confiance - en général, lorsque quelque chose vous semble plutôt étrange ou louche, suivez votre intuition.
- En cas de doute, vérifiez la source et signalez-la.

# 15. Vol d'identité

Le vol d'identité est l'usurpation délibérée de l'identité d'une autre personne, habituellement pour accéder à son information financière, faire des achats à ses frais ou la faire accuser d'un crime qu'elle n'a pas commis. Il y a vol d'identité lorsque vous vous faites voler des renseignements personnels, comme votre date de naissance, votre numéro d'assurance sociale, votre passeport, votre adresse, votre nom et les renseignements sur votre compte en banque, généralement sans que vous le sachiez. Les cas d'identité volée pour l'immigration illégale, le terrorisme, l'espionnage ou pour un changement d'identité permanent sont plus rares.

Pour obtenir d'autres détails sur le vol d'identité et sur la façon de le prévenir, vous pouvez visualiser la présentation PowerPoint suivante sur le site Web intranet de la section de la sécurité informatique : Protégez votre identité - Empêcher le vol d'identité.



# 16. Signalement des incidents de sécurité

Un incident de sécurité signifie qu'il y a eu, par exemple :

- Vol, perte ou destruction de revenus, d'argent, de biens saisis ou retenus, ou d'autres biens appartenant à l'ASFC ou sous le soin de celle-ci.
- Abus, menaces, harcèlement criminel et voies de fait contre les employés.
- Compromission soupçonnée ou réelle de renseignements protégés et/ou classifiés.
- Envoi de programmes malveillants ou alertes/attaques virales contre les systèmes informatiques ou de communication de l'ASFC ou autres circonstances menant à la dégradation du fonctionnement du système (ne transférez pas des fichiers ou des messages si vous pensez que votre ordinateur est infecté, appelez le service de dépannage de TI).
- Perte, vol ou emploi abusif de cartes d'identification/accès, de passes pour entrer dans un édifice, de cartes d'autorisation et de clés.
- Des incidents ayant des répercussions sur la sécurité matérielle d'un édifice ou d'installations de l'ASFC causant la fermeture ou l'évacuation à la suite, entre autres, de pannes de courant, d'incendies, de vandalisme, d'inondation ou d'accidents météorologiques.
- Des incidents que l'on soupçonne d'être des activités inacceptables ou illicites ou des infractions criminelles.
- Des incidents qui ont des répercussions sur les activités du gouvernement ou qui pourraient nécessiter la modification des normes opérationnelles ou des documents techniques.

Vous pouvez obtenir d'autres détails sur le signalement des incidents de sécurité dans le site intranet sur la sécurité de l'Agence.

Ce document fut élaboré par la Sécurité des TI de la Direction générale de l'innovation, des sciences et de la technologie en collaboration avec la Sécurité de l'agence et des affaires internes de la Direction générale du contrôle.

Canada Border Services Agency | Agence des services frontaliers du Canada



# CBSA IT Security Guidelines On Device and Information Security While on International Travel

## About this Guideline

The Guideline on Device and Information Security While on International Travel (the Guideline) provides guidance to CBSA employees while travelling abroad as well as functional specialists responsible for preparing IT devices for said travel.

This guideline is based on the advice and guidelines published by the Communication Security Establishment Canada (CSE) and Public Safety Canada.

## 1. Introduction

Mobile technology devices such as BlackBerry, laptops, and tablets are key enablers for operational efficiency and vital to the modern workforce; however, they are also susceptible to security threats.

International travelers can also find additional information on the CBSA's Atlas page International Travel and Protocols.

## 2. Security Considerations

Government employees travelling outside of Canada face increased Information Technology (IT) security risks. Employees should carefully consider the risks of using a mobile device during travel.

Considerations:

- Senior management personnel may be at higher risk of being targeted through their mobile technology devices;
- Mobile technology devices can be compromised in a number of ways - even remotely;
- In some countries, hotel business centers and phone networks are monitored and in some locations, rooms may even be searched. As a general guideline, assume that there is no expectation of privacy in offices, hotels, internet cafes, or other public areas;
- Mobile technology devices are a prime target for theft. If stolen, the information contained within may be accessed and used for malicious purposes.

## 3. Recommendations for International Travel (Outside of Canada)

To mitigate security risks, the following is recommended:



- Employees should be issued a travel inventory device (BlackBerry, tablet [i.e. iPad], laptop) that will be returned after travel:
- Check the Travel.gc.ca site for travel advisories or request an up-to-date security brief for the country of destination directly from CSIS. Contact the CSIS Government Liaison Office at to determine if such a briefing is available and/or required:
    - CSIS can provide a brief on the latest espionage and eavesdropping techniques, including remote laser listening and associated gadgets as well as how to mitigate the risks;
    - CSIS should provide information as to the acceptability of cryptography for the specific countries to be visited. For example, it may be illegal in some countries to have GPS tracking enabled or they may require that they supply SIM cards. This information must be shared with IT Support before you obtain your travel device.
- In certain countries, mobile technology devices can be legally seized (temporarily or permanently) where employees will be obligated to provide login and password information to unlock them. A new and separate password, from any CBSA network account, should be used on the travel device;
- Unless absolutely necessary, avoid taking mobile technology devices to high risk countries. The Travel.gc.ca link (above) can assist in determining high risk countries or, for additional guidance, contact the CSIS Government Liaison Office at (613) 842-1110;
- Consider using diplomatic courier service for the shipment of mobile technology device(s):
    - If the employee is travelling to a low risk country and then going to a high risk country, it is recommended that the employee make arrangements via diplomatic courier to send the device(s) back to Canada before departing for the high risk country;
    - If the employee is travelling to a high risk country first and then going to a low risk country, it is recommended that the device(s) be delivered directly to the low risk country via diplomatic courier in order to avoid said device(s) crossing into the high risk country;
- File handling - while information can be stored on a device, **no important or sensitive information** may be stored on the device;
- USB keys must not be used;
- Audio, video and SMS text messaging functions of the device may be used, if necessary; however, **no important or sensitive information** may be transmitted;
- PIN-to-PIN on BlackBerry devices must not be used;
- The device must be turned off when not in use;
- Devices must not be connected to or used near Field Communications or Wi-Fi hotspots;
- Consider using a commercial service to avoid any connection to the Agency's network; and
- Upon return, report to the Departmental Security Officer and IT Security immediately if a device(s) was seized or outside of the user's possession at any time. Information on Security Incident Reporting can be found at the following link: http://atlas/cb-dgc/pol/cm-mc/sv-vs/psd-dsm/sir_sis_eng.asp.

# 4. Roles and Responsibilities

The IT Security and Continuity division (CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca) provides security guidance on the use of technology assets.

The Infrastructure and Information Security Division (information_security-securite_de_linformation@cbsa-asfc.gc.ca / CBSA-ASFC_DSO_Physical_Security-Securite_Materielle) provides advice on information and physical security.



The Headquarters IT Support Services team (CBSA-ASFC_IT-Requests@cbsa-asfc.gc.ca) will set up travel devices as requested and will provide operational IT support service for CBSA HQ personnel. See Appendix A.

The CRA Regional IT Support Services team will configure travel devices as requested as well as provide operational IT support service for CBSA regional employees. See Appendix A.

## 5. Enquiries

For questions on the content of this guideline, please contact the IT Security and Continuity division (CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca).

## Appendix A: Notes for IT Support

- Travel devices should be configured with only the minimum data required for the trip:
  - ensure applications installed on the mobile devices have the most recent patches installed;
  - disable unnecessary features (Wi-Fi, infrared ports, Bluetooth, PIN-to-PIN);
  - update the web browser with strict security settings;
  - implement a locked-down travel profile on the BlackBerry Enterprise Server (for BlackBerry devices);
  - the Secure Remote Access (SRA) connection should not be configured - exceptions include the "5 Eye Group of Countries"; and
  - change the BitLocker password and advise the employee.
- Prepare for incident handling:
  - increase logging and monitoring capabilities; and
  - image the device using a mobile device management (MDM) application to allow for comparisons post travel.
- Consider using diplomatic courier service for the shipment of mobile technology devices.
- When the employee returns:
  - recall travel inventory device;
  - report to IT Security and the DSO immediately if the device(s) was seized or outside the user's possession at any time; and
  - re-image the device and dispose of the SIM card as per Agency procedures (following security incident reporting).

## Appendix B: Additional resources / references

- Mobile Technologies in International Travel - Guidance for Government of Canada Business Travelers (ITSB-87)
- Mobile Technologies in International Travel - Guidance for Government of Canada IT Security Managers (ITSB-88)
- Remaining Cyber Safe While Travelling: Security Recommendations
- International use of cryptography
- Scams and fraud





- Laptop Travel Guidelines
- Cyber Security Consumer Tips for International Travel
- Advanced Persistent Threat:
  http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-eng.aspx
  http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/AL11-003-eng.aspx
- Travel Information and Advisories



# Directive sur la sécurité de la TI de l'ASFC visant la sécurité des appareils et de l'information lors des voyages internationaux

## À propos de la présente directive

La Directive sur la sécurité de la TI de l'ASFC visant la sécurité des appareils et de l'information lors des voyages internationaux (la Directive) fournit une orientation aux employés de l'ASFC qui voyagent à l'étranger de même qu'aux spécialistes fonctionnels chargés de préparer les appareils de TI de ces employés voyageant à l'étranger.

La Directive se fonde sur les conseils et les lignes directrices qui ont été publiés par le Centre de la sécurité des télécommunications Canada (CSTC) et par Sécurité publique Canada.

## 1. Introduction

Les technologies mobiles telles que les BlackBerry, les ordinateurs portatifs et les tablettes constituent des incontournables pour l'efficacité opérationnelle et sont devenus indispensables aux travailleurs d'aujourd'hui; toutefois, ces technologies sont également vulnérables aux menaces.

Les voyageurs internationaux peuvent également trouver des renseignements supplémentaires sur la page Atlas des voyages internationaux et des protocoles.

## 2. Considérations liées à la sécurité

Les employés du gouvernement qui voyagent à l'extérieur du Canada font face à des risques accrus en matière de sécurité des technologies de l'information (TI). Les voyageurs doivent bien évaluer les risques potentiels liés à l'utilisation de leur appareil mobile durant leurs déplacements.

Points importants à considérer :

Les personnes occupant des postes de cadres supérieurs ont plus de risques que leurs appareils de technologie mobile soient ciblés;
Les appareils de technologie mobile peuvent être compromis de bien des façons - même à distance;
Dans certains pays, les centres d'affaires dans les hôtels ainsi que les réseaux téléphoniques sont surveillés et les chambres d'hôtel peuvent même être fouillées. En règle générale, on ne doit s'attendre à aucun respect de la vie privée dans les bureaux, les hôtels, les cafés Internet ou tout autre endroit public;
Les appareils de technologie mobile sont des cibles de choix pour les voleurs qui pourraient accéder aux informations qu'ils contiennent et les utiliser à des fins malveillantes.

# 3. Recommandations liées aux voyages internationaux (à l'extérieur du Canada)

Afin d'atténuer les risques en matière de sécurité, les mesures suivantes sont recommandées :

Les employés devraient se procurer un appareil de voyage (BlackBerry, tablette [p.ex., un iPad], ordinateur portatif) qu'ils remettront à leur retour.

Consultez les avertissements aux voyageurs en visitant le site Voyage.gc.ca ou demandez directement auprès du SCRS un avis de sécurité à jour sur le pays de destination. Contactez le Bureau de liaison gouvernementale du SCRS en composant le 613 842 1110 pour déterminer si un avis de sécurité est disponible et/ou est nécessaire :

- Le SCRS peut fournir de l'information sur les plus récentes techniques d'espionnage et d'écoute clandestine, y compris l'écoute à distance par faisceaux laser et les gadgets associés, ainsi que des conseils sur les façons d'atténuer les risques;
- Le SCRS fournit de l'information quant à l'acceptabilité de la cryptographie pour les pays étrangers. Par exemple, il peut être illégal dans certains pays d'activer la fonction GPS ou ils peuvent exiger que des cartes SIM spécifiques soient utilisées. Cette information doit être partagée avec le support des TI avant d'obtenir l'appareil de voyage.

Dans certains pays, les appareils de technologie mobile peuvent être saisis légalement (de façon temporaire ou permanente) et, dans un tel cas, les voyageurs doivent fournir leurs codes d'utilisateur et mots de passe pour déverrouiller leurs appareils.

Un mot de passe nouveau et différent de tout autre compte réseau de l'ASFC devrait être utilisé sur l'appareil de voyage;

Éviter d'emporter des appareils de technologie mobile dans des pays à risque élevé, sauf s'il est absolument nécessaire de le faire. Le lien à la page Travel.gc.ca (ci-dessus) peut vous aider à déterminer les pays à risque élevé ou, pour de plus amples conseils, communiquez avec le Bureau de liaison gouvernementale du SCRS en composant le

Considérer le recours à un service de courrier diplomatique pour l'expédition des appareils de technologie mobile :

- Si un employé se rend dans un pays à faible risque et doit ensuite voyager dans un pays à risque élevé, il est recommandé qu'il prenne des arrangements avec un service de courrier diplomatique pour retourner son ou ses appareils au Canada avant de se rendre dans le pays à risque élevé;
- Si un employé se rend d'abord dans un pays à risque élevé et va ensuite dans un pays à faible risque, il est recommandé qu'il prenne des arrangements avec un service de courrier diplomatique pour que son ou ses appareils lui soient livrés directement dans le pays à faible risque pour éviter que les appareils ne se trouvent à l'intérieur du pays à risque élevé;



Traitement des fichiers - Bien qu'il est possible de stocker des renseignements sur un appareil, il ne faut stocker **aucun renseignement important ou de nature délicate** sur les appareils;
Les clés USB ne doivent pas être utilisées;
Les fonctions audio, vidéo et de messagerie texte de l'appareil peuvent être utilisées, au besoin; toutefois, **aucun renseignement important ou de nature délicate** ne doit être divulgué;
Le service NIP à NIP sur les appareils BlackBerry ne doit pas être utilisé;
Les appareils doivent être éteints lorsqu'ils ne sont pas utilisés;
Les appareils ne doivent pas utiliser la communication en champ proche ou se connecter à des points d'accès sans fil Wi-Fi;
Considérer faire appel à un fournisseur de services commercial pour éviter toute connexion avec le réseau du ministère; et
Au retour, il faut signaler tout de suite à l'agent de sécurité du Ministère et à la Sécurité des TI si le ou les appareils ont été saisis ou n'ont pas été en tout temps en la possession de l'utilisateur. De l'information sur le signalement des incidents de sécurité est disponible au lien suivant : http://atlas/cb-dgc/pol/cm-mc/sv-vs/psd-dsm/sir_sis_fra.asp.

# 4. Rôles et responsabilités

La Division de la sécurité et de la continuité des opérations des TI (CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca) fournit des directives de sécurité à l'égard des biens technologiques.

La Division de la gestion de la sécurité matérielle et de l'infrastructure (information_security-securite_de_linformation@cbsa-asfc.gc.ca / CBSA-ASFC_DSO_Physical_Security-Securite_Materielle) fournit des conseils sur la sécurité de l'information et la sécurité matérielle.

L'équipe des Services de soutien de la TI à l'Administration centrale (CBSA-ASFC_IT-Requests@cbsa-asfc.gc.ca) configurera des appareils de voyage sur demande et offrira un service de soutien opérationnel de la TI au personnel de l'AC de l'ASFC. Voir l'annexe A.

L'équipe régionale des Services de soutien de la TI de l'ARC configurera des appareils de voyage sur demande et offrira également un service de soutien opérationnel de la TI aux employés régionaux de l'ASFC. Voir l'annexe A.

# 5. Demandes de renseignements

En cas de questions sur le contenu de la présente directive, veuillez communiquer avec la Division de la sécurité et de la continuité des opérations des TI (CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca).

# Annexe A : Notes pour le Soutien de la TI







Les appareils de voyage devraient être configurés de manière à ne contenir que les données minimales requises durant le voyage :

- s'assurer que les applications installées sur les appareils mobiles ont été mises à jour au moyen des correctifs les plus récents;
- désactiver les fonctions non nécessaires (Wi-Fi, ports infrarouges, Bluetooth, NIP à NIP);
- actualiser le navigateur Web en établissant des paramètres de sécurité stricts;
- procéder au verrouillage du profil de voyageur sur le serveur d'entreprise BlackBerry (pour les appareils BlackBerry);
- la connexion d'accès à distance protégé (ADP) ne devrait pas être configurée - à l'exception des pays du « Groupe des cinq »; et
- changer le mot de passe du BitLocker et en informer l'employé.

Précautions pour le traitement des incidents :

- augmenter les capacités de journalisation et de surveillance; et
- créer l'image de l'appareil à l'aide d'une application de gestion des appareils mobiles pour pouvoir faire des comparaisons après les déplacements.

Considérer recourir à un service de courrier diplomatique pour l'expédition des appareils mobiles.

Au retour de l'employé :

- récupérer l'appareil de voyage;
- signaler tout de suite à la Sécurité de la TI et à l'agent de sécurité du Ministère si le ou les appareils ont été saisis ou n'ont pas été en tout temps en la possession de l'utilisateur; et
- recréer l'image de l'appareil et supprimer la carte SIM conformément à la procédure de l'Agence (après le signalement d'un incident).

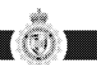
# Annexe B : Ressources supplémentaires/Références

Technologies mobiles pour les voyages internationaux - Conseils pour les employés du gouvernement du Canada en voyage d'affaires (ITSB-87)
Technologies mobiles pour les voyages internationaux - Conseils pour les gestionnaires en sécurité des TI du gouvernement du Canada (ITSB-88)
Cybersécurité au cours des déplacements : Recommandations en matière de sécurité
Utilisation internationale de la cryptographie
Escroqueries et fraudes
Directives sur les déplacements avec un ordinateur portable (en anglais seulement)






Agence des services frontaliers du Canada	Canada Border Services Agency



Conseils aux consommateurs sur la cybersécurité lors des voyages internationaux (en anglais seulement)
Menaces sophistiquées et persistantes :
http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-fra.aspx
http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/AL11-003-fra.aspx
Informations relatives aux voyages et avertissements

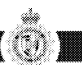
Canada Border Services Agency | Agence des services frontaliers du Canada



# Directive on the Appropriate Use of Electronic Mail (E-mail)

PROTECTION • SERVICE • INTEGRITY

Canada



# 1. Effective Date

This directive is effective immediately upon issuance.

This directive, formerly a policy, replaces version 1.1 (January 4, 2010) and incorporates administrative updates effective May 13, 2013.

# 2. Directive

The Canada Border Services Agency (CBSA) directive on the appropriate use of electronic mail (e-mail) is based on the CBSA Policy on the Use of Electronic Resources. This directive expands and further elaborates upon the security requirements for the use appropriate use of email referred to in the CBSA Policy on the Use of Electronic Resources.

# 3. Directive Objective

The purpose of this directive is to ensure the appropriate use of CBSA's e-mail services by authorized individuals in accordance with Government of Canada laws, policies, standards and guidelines, as well as CBSA's policies, standards and guidelines.

This directive also intends to inform all CBSA authorized users of their obligations and responsibilities with respect to the appropriate and authorized use of CBSA's e-mail system.

# 4. Scope and Application

This directive applies to:

1. all e-mail services provided by CBSA;
2. all authorized individuals who access CBSA's e-mail system.

This directive requires all authorized individuals to read and understand the CBSA Policy on the Use of Electronic Resources.

# 5. Context



CBSA uses the e-mail system as a business communication tool that is critical to the daily operations and business of the Agency. Authorized individuals must use this tool in a responsible, effective and lawful manner that promotes and supports the mandate of CBSA.

Users of the e-mail system must be aware that they are accountable for all electronic messages they create, send or receive[1] through CBSA's e-mail system.

E-mail remains stored on CBSA informatics equipment even after the originator or recipient has deleted the message. Once e-mail is outside the Canada Revenue Agency (CRA) and Shared Services Canada (SSC) firewalls, gateways or systems, it is not secure from interception or alteration, unless encrypted. Corporate messages created, received or distributed via CBSA's e-mail system are the property of the Canada Border Services Agency and must be managed as government information assets.

## 6. Definitions

**Access**

means gaining entry to or using the e-mail resources that CBSA provides to authorized individuals. Access to such resources may be from inside or outside government premises. Access supports telework and remote access situations or where authorized individuals are using e-mail services provided by CBSA on their own time for limited personal use as defined in this directive and CBSA's Policy on the Use of Electronic Resources.

**Authorized individuals**

include CBSA employees, contractors / consultants and all other persons who have been authorized by management to access CBSA's electronic resources and its e-mail services.

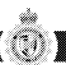
**Electronic mail (e-mail)**

includes all electronic messages and transmissions created, stored, received and distributed via CBSA's e-mail system, including portable and wireless devices. CBSA's e-mail systems and services include the corporate e-mail systems and services, and other CBSA authorized e-mail services. E-mail, for the purposes of this directive, always includes all infrastructure and e-mail services provided for CBSA by CRA and SSC.

**Monitoring of E-mail**

means any action that involves the recording and subsequent analysis of activity or use of services as defined in this directive and the CBSA Policy on the Use of Electronic Resources.

For additional definition of terms, refer to Annex C of this document or the ISTB Glossary. (Enter IT Security to return IT Security terms only).



# 7. Directive Statement

It is the CBSA policy that authorized individuals use Agency approved e-mail services to conduct the business of government. This could include communication with other government employees, to communicate with the public, to gather information relevant to their duties on a need-to-know basis, and to develop expertise in using such resources.

E-mail services provided for and by CBSA are for business purposes. Limited personal use is permitted if it complies with CBSA's Policy on the Use of Electronic Resources as well as all other applicable CBSA, federal and provincial policies and legislation. E-mail services are subject to monitoring and Access to Information and Privacy (ATIP) requirements and requests.

# 8. Directive Requirements

CBSA e-mail is subject to all legislation governing written communications, including the *Access to Information Act*, the *Privacy Act*, the *Library and Archives of Canada Act*, the *Official Languages Act*, the *Canadian Human Rights Act*, the *Criminal Code* and the *Values and Ethics Code for the Public Service*.

Under the *Access to Information Act* and the *Privacy Act*, individuals may have access to electronic records, subject to applicable exemptions under those acts.

# 9. Authorized Use of E-mail

E-mail services shall be used for official business to carry out the mandate and mission of CBSA. Only CBSA supported and approved e-mail services and systems, including all devices capable of any type of electronic messaging, are to be used. No other e-mail providers / systems (for example, Hotmail, GMail, Yahoo Mail, a user's personal service provider) are to be used. Authorized individuals who use CBSA e-mail services must observe the prohibitions against criminal, unlawful and unacceptable activities outlined in CBSA's Policy on the Use of Electronic Resources and this directive and must comply with all related legislation, policies and guidelines.

CBSA's electronic e-mail services are to be used for approved purposes, namely:

1. Conducting government business such as:
   - communicating and sharing information with colleagues, other government departments and the private sector in the performance of CBSA functions and activities;
   - gathering information relevant to a user's duties;
   - announcing group events that are authorized and supported by CBSA management, such as fundraising for a charitable campaign;

   - using distribution lists to transmit information for business purposes;
   - undertaking professional development activities that are job related.
2. Limited personal use (during lunch break, periods of rest or after work, and activities, as specified in the CBSA Code of Conduct), such as:
   - communicating with family, friends and other persons for other than official purposes;
   - accessing acceptable news and other information sources that are not prohibited or restricted by law or policy;
   - conducting routine personal banking transactions;
   - any union activity or business that is not prohibited or restricted by law or policy.
3. Any other purpose that is consistent with the Treasury Board's Policy on the Use of Electronic Networks, CBSA's Policy on the Use of Electronic Resources and this directive, or that is specifically authorized in writing by management.

All uses of e-mail services for activities such as special events and distribution lists require prior approval by management.

## Conditions of Limited Personal Use

Limited personal use is permitted on e-mail systems on condition that it complies with all applicable CBSA, federal and provincial policies and legislation.

The limited personal use of CBSA's e-mail resources by authorized individuals must not:

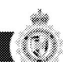
1. Interfere with a user's productivity or the performance of their official duties and functions.
2. Incur any direct costs to the Agency.
3. Involve a criminal, unlawful or unacceptable activity as defined in the CBSA Policy on the Use of Electronic Resources.
4. Impose a performance or storage burden on the Agency's electronic resources.

## Use of E-mail for Union Business

Use of e-mail for union notices or other union material requires prior approval of CBSA Labour Relations.

E-mail for union business:

1. Can be used to communicate with management, Human Resources, Labour Relations and the Informal Conflict Management System (ICMS).



2. Must not be used to communicate generally to union membership unless explicit authorization has been obtained from management.
3. Can be used by union representatives to contact an employee to answer individual requests, such as a grievance or other employee / management issues.
4. Must be in accordance with an employee's right to privacy and the content of such e-mails should not be considered by the Agency as adverse to the interests of the Agency or any of its representatives.

Union representatives are accountable for all electronic messages they generate or distribute from their CBSA account.

## Protection of E-mail Communications

E-mail sent outside the Government of Canada network is not secure. Therefore, users should exercise caution about the content of messages they send outside the Government's mail system.

E-mail communications must be protected in the following manner when they are transmitted across the CBSA / CRA standard network[2], to an identified recipient of a federal government department or agency, or outside the Agency.

1. Unclassified information can be transmitted with no additional controls, such as encryption.[3]
2. Protected A information can be transmitted with no additional controls, such as encryption, except where a Threat and Risk Assessment (TRA) recommends encryption for information at the Protected A level.
3. All Protected B information must be encrypted.
4. Protected C or Classified information must not be transmitted via the standard e-mail system.

## Corporate and Transitory Information

All e-mail messages, including attachments, that are created, received or transmitted in the normal course of CBSA operations and that contain information on CBSA functions, actions and decisions must be preserved. All users are therefore responsible for the effective management of all e-mail messages they create and receive via their e-mail mailboxes. E-mail messages are considered official records of CBSA. They must be preserved and protected from unauthorized destruction and access. Refer to Annex A of this directive defining Corporate and Transitory Information. Further details can be obtained from the CBSA Policy on the Information Management Program and the Treasury Board Secretariat Management of Government Information (MGI) Policy.

## Other Considerations



E-mail shall not be used to create, store, transmit or solicit4 inappropriate, unlawful and unacceptable activities such as chain letters, pornography, etc.

Communication involving use of e-mail resources, including Internet use, will be monitored.

E-mail communications must not be inflammatory, harassing, defamatory or disruptive to the Government of Canada, CBSA, external partners, organizations or individuals.

All information, including e-mail, must be properly identified and labelled in accordance with the CBSA Security Policy, Chapter 5, Identifying Classified and Protected Information and Assets.

Unsolicited e-mails, often referred to as SPAM, are to be deleted unless the e-mail contains extremely offensive, unlawful, or criminal material.

Additional information regarding non-agency e-mail accounts, automatic forwarding of e-mail messages, wireless e-mail and generic e-mail accounts can be found under the following security policies: Chapter 17, Access Accountability and Authentication to Agency Information Technology Systems and Chapter 23, Communication Security (COMSEC).

Refer to Annex B for additional information regarding spam messages.

## 10. Criminal, Unlawful, and Unacceptable Activities

CBSA's e-mail services shall not be used to conduct criminal, unlawful or unacceptable activities as defined in the CBSA Policy on the Use of Electronic Resources and all other applicable policies.

A non-comprehensive list of these types of activities is included in Annexes A, B and C of CBSA's Policy on the Use of Electronic Resources.

## 11. Roles and Responsibilities

### Authorized Individuals

All individuals who access CBSA's e-mail must adhere to this directive and to all applicable government policies and laws, and will be held accountable for all activities they perform using CBSA's e-mail services.

Authorized individuals accessing and using CBSA's e-mail services are responsible for:

1. Ensuring that they use CBSA's e-mail system for government business and for purposes authorized by management.







2. Managing e-mail messages in accordance with CBSA's records management guidelines.
3. Reporting the receipt of any e-mail that does not comply with this directive immediately to their supervisor, who will ensure that it is actioned at the appropriate level.
4. Encrypting all communications containing Protected B sensitive information (as described in this directive under the section Protection of E-mail Communications).
5. Digitally signing communications, when required, containing Protected A or Protected B sensitive information to provide authentication of e-mail messages.[5]
6. Ensuring that under no circumstances Protected C or Classified information is to be transmitted by the standard e-mail system.

## Managers

Managers must ensure that users are aware of this e-mail directive. As well, they must ensure that users have read and understood CBSA's Policy on the Use of Electronic Resources.

Managers are responsible for reporting instances of suspected criminal, unlawful or unacceptable uses of CBSA's e-mail to the Director of Information Technology Security or to the Security and Professional Standards Directorate (SPSD).[6]

## Departmental Security Officer (DSO)

The DSO reserves the right to grant access to a user's e-mail as part of a formal investigation or to meet Agency business requirements. Written approval must be provided and the procedures of how the information was accessed must be recorded.

The Departmental Security Officer is responsible for:

1. Referring managers to Security and Professional Standards Directorate for requests involving accessing e-mail messages or files located in a user's account.
2. Referring managers to Security and Professional Standards Directorate when there is suspected misuse of the Agency's electronic resources.
3. Investigating reports of suspected criminal, unlawful or unacceptable uses of CBSA's e-mail services.
4. Seeking advice from Labour Relations and Legal Services in cases of suspected criminal and / or unlawful uses of CBSA's e-mail resources and reporting to law enforcement authorities, when necessary.
5. Responding to any requests pertaining to the Access to Information Act that are relevant to this directive.

## Labour Relations



Labour Relations may provide guidance to Security and Professional Standards in support of any investigation that is undertaken into the unlawful or unacceptable use of the e-mail system.

## 12. Privacy and Monitoring

### Expectations of Privacy

The Canadian Charter of Rights and Freedoms guarantees that government authorized individuals have a right to a reasonable expectation of privacy, and this right extends to the workplace.

Copies of files and e-mail records (including deleted records) are automatically backed up and retained on a daily basis. This information may be accessible under the *Access To Information Act* and *Privacy Act*, subject to exemptions under those Acts.

### Monitoring of E-mail

The Security and Professional Standards Directorate is the functional authority for content monitoring. The content monitoring function may include, but is not limited to, viewing the content and analyzing the volume of files, e-mails or logs where there are grounds to suspect misuse.

If there are grounds to suspect that an individual is misusing the Agency's electronic resources, due to a routine analysis[7] or a complaint, the matter shall be referred to Security and Professional Standards Directorate for further investigation. They can authorize monitoring, with or without prior notification to the individual, including reading or viewing the content of individual e-mail records or other files.

Monitoring may also be conducted on a random basis in accordance with the *Canadian Charter of Rights and Freedoms*, the *Privacy Act* and the *Criminal Code*.

## 13. Disciplinary Measures

Individuals who violate this directive are subject to disciplinary action up to and including termination of employment, as outlined in the CBSA Policy on the use of Electronic Resources.

## 14. Directive Review



This directive document shall be reviewed at least every five years under the authority of the Director General, Infrastructure Services, the Director General, Security and Professional Standards Directorate, and the Departmental Security Officer (DSO).

## 15. References

## Related Legislation and Policies

- CBSA Code of Conduct
- Value and Ethics Code for the Public Service
- CBSA Discipline Policy and Discipline Guidelines
- CBSA Communication Security (COMSEC) Policy
- CBSA Policy on the Use of Electronic Resources
- CBSA Guidelines for the Policy on the Use of Electronic Resources
- CBSA Security Policies
- CBSA Management of Electronic Mail - Policy
- CBSA Management of Electronic Mail - Guidelines and Procedures
- *Financial Administration Act*
- *Access to Information Act*
- *Privacy Act*
- *Charter of Rights and Freedoms*
- *Library and Archives of Canada Act*
- *Security of Information Act*
- *Criminal Code*
- *Crown Liability and Proceedings Act*
- *Copyright Act*
- *Trade-Marks Act*
- *Canadian Human Rights Act*
- *Official Languages Act*

## Cross-References

Treasury Board Policy and Publications

- Prevention and Resolution of Harassment in the Workplace
- Policy on Government Security
- Government Communications Policy
- Government of Canada Internet Guide
- Management of Government Information Policy (MGI)
- Management of Information Technology Security (MITS)
- Directive on Losses of Money or Property
- Privacy and Data Protection Policy
- TBS Policy on the Use of Electronic Networks
- Telework Policy
- Guidelines for Discipline TBS



## 16. Enquiries

Enquiries regarding this directive should be directed to:

Information, Science and Technology Branch
IT Security and Continuity
Email: IT Security and Continuity
Intranet: IT Security

Comptrollership Branch
Security and Professional Standards Directorate
Email: Security and Professional Standards Directorate

## Annex A — Corporate and Transitory Information

The following guidelines apply to all authorized users who create, receive, use, or transmit information using the CBSA e-mail system.

Corporate information — information recorded in any form, including data in computer systems; paper or electronic documents such as correspondence, memoranda, plans, maps, and drawings; sound recordings; e-mail messages; electronic images; and any other documentary materials created or received by an organization or person conducting official business.

- Messages that reflect the position or business of the CBSA.
- Messages that initiate, authorize, or complete a business transaction.
- Messages received from external sources that are clearly of interest to the CBSA in the conduct of its business.
- E-mail drafts that show the evolution of a document through the approval processes.
- Copies containing more or less information than the original record.
- Original messages of policies or directives.
- Original postmaster messages.

If the information does not exist elsewhere:

Messages related to work schedules and assignments.
Agenda and minutes of meetings; briefing notes.
Final reports and recommendations.

### E-mail identified as corporate information must be retained



Transitory information — information that is required only for a limited time to ensure a routine action is completed or a subsequent record is prepared. Transitory information does not include information required by government institutions or ministers to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities.

## E-mail you identify as transitory information should be deleted when it is no longer of use, for example:

- Messages that are copies of information used only for reference and not as the official record.
- Messages in a form used for casual communication.
- Informal messages or rough drafts that are not required as evidence in the development of a document; messages that are duplicate copies of information.
- Miscellaneous notices of employee meetings, holidays, etc.
- Messages received as part of a distribution list and other Internet sources, solely for convenience of reference.
- Duplicate copies used for information or reference purposes only where any additional information has been incorporated into subsequent versions.
- Rough or working drafts that are not required to document the steps in the evolution of a document.
- Information not related to the CBSA's business such as announcements or unsolicited advertising from sources outside the CBSA.

Note: You must not delete e-mail that contains transitory information after you receive a formal request under the *Access to Information Act* or *Privacy Act* relating to that information. At the time of such a request, all existing information must be considered for possible release, regardless of whether or not it is transitory. The list above provides examples; it is not a complete list of all information that you must keep.

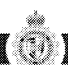
# Annex B — Spam Messages

Spam messages are unwanted, unsolicited e-mail messages received from an external address. Most spam messages are advertisements and should be deleted. However, some spam messages may include extremely offensive, unlawful, or criminal material, such as child pornography and scams, and must be reported.

Examples of spam messages to delete:

Advertisements for pills, software, jewellery, supplies, courses or training, dating services and stock / investments alerts.
Messages asking for or offering employment.

Examples of spam messages to report:



Messages containing images of child pornography or any advertisements or Internet links to that effect.
Requests for personal information, such as credit card numbers or online banking user ID and password (phishing).
Messages containing pornographic material.
Messages involving pyramid schemes schemes.

If a spam message is considered a security incident, contact your local IT support desk and the Security and Professional Standards Directorate of the Comptrollership Branch.

## Annex C — Terms and Definitions

This annex sets out an alphabetical list of terms and explanations found in this directive as well as the CBSA Policy on the Use of Electronic Resources. This serves as a reference guide to help users better understand the provisions of these policies.

**Assets**

are tangible or intangible things of the Government of Canada. Assets include, but are not limited to, information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.

**Availability**

is the condition of being usable on demand to support operations, programs and services.

**Chain letters**

are e-mail messages with a single intent - to have you forward them to others. They falsely offer luck, money or a wish if you send them on.

**Chat rooms**

are electronic forums where participants can have online chat discussion in real time, normally through the exchange of text messages with each other in real time.

**Classified information**

is information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest. See also Sensitive Information.

**Compromise**

includes injury due to unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

**Confidentiality**

is the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to



national or other interests, with reference to specific provisions of the Access to Information Act and the Privacy Act.

**Content administration**

may include, but is not limited to, installing out of office messages or extracting corporate documents.

**Content monitoring**

may include, but is not limited to, viewing the content and analyzing the volume of files, e-mail messages or logs to determine whether misuse has occurred.

**Electronic resources**

Groups of computers, computer networks and systems, functions, or devices allocated to users or programs. Without restricting the generality of the foregoing, these resources include the Internet, functions, software or devices internal to CBSA, and public and private functions or devices external to the Agency. Also included are any hardware such as standalone computers, laptops, peripherals, memory devices, wireless devices, and any other media used to obtain, store, disseminate information, etc. Many non-computing devices, such as digital cameras and cellular phones, are considered as electronic resources under this directive because of their capability for storing and disseminating information. Electronic resources, for the purposes of this directive, always include infrastructure and network services provided to CBSA by the Canada Revenue Agency (CRA) or Shared Services Canada (SSC) and network services between CBSA and other government organizations.

**Gambling**

means to bet, wager or risk money or something of value on a game of chance or mixed skill and chance. It may take many forms and includes sports pools and other types of pools.

**Information**

is a corporate asset or resource, which is defined as data, facts or knowledge that is recorded, regardless of form, recording media or technology used.

**Information technology security**

involves safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

**Integrity**

is the accuracy and completeness of assets and the authenticity of transactions.

**Misuse**

means any action or inaction by a user that constitutes an unacceptable activity, an unlawful activity or a criminal activity.

**Nudity**

is a naked person or a person displaying genitalia. Does not need to be sexual in content.

**Offensive material**

is likely to insult, disgust or repulse. These include jokes made against select groups (e.g. racial, religious, or sexist jokes). It



may also include offensive images (e.g. images of corpses, portrayals of defecation).

**Phishing**

is a form of Internet fraud that uses authentic-looking but false e-mails, websites or other information in order to steal valuable information such as credit cards, social insurance numbers, user IDs and passwords.

**Pornography**

is explicitly sexual material designed or intended to cause sexual arousal or titillation.

**Primary systems**

are databases such as CAS, mainframe applications and network applications. They are provided for Agency business purposes only.

**Private business**

is an activity outside the scope of employment conducted for personal gain or profit. This includes the sale or purchase of any goods or services. This category also includes the conduct of political activity.

**Profanity**

includes material where vulgar (offensive) language is used. It includes, but is not limited to, vulgar language in a written text, oral use of the words in a sound file or video, or even a caption with an image.

**Protected information**

is information related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to a non-national interest. See also Sensitive Information.

**Pyramid schemes**

are hierarchies in which you are encouraged to send money with the expectation that a set number of individuals will in turn send you money.

**Records**

are information in any physical or electronic form, including audio-visual records, photographs, maps, drawings, film, sound recording, videotape, microform, magnetic tape, paper or electronic files, and any other documentary material.

**Risk**

is the chance of a vulnerability being exploited or resulting in harm.

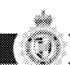
**Secondary systems**

are comprised of applications such as e-mail, Microsoft Office and Internet (where limited personal use is permitted).

**Security incident**

is compromise of an asset, or any act or omission that could result in a compromise; threat or act of violence toward employees.

**Sensitive information**



is information that must be afforded appropriate safeguards because of its confidential nature. See also Classified information and Protected information.

**Sexual content**

is material where the sexual act may not be explicit (detailed) but intent to cause sexual arousal or titillation is present. It is evident that a mature sexual theme is being displayed or described.

**Spam messages**

are unwanted, unsolicited e-mail messages received from an external address. Most spam messages are advertisements; however, some could also include messages with criminal content, such as child pornography and scams.

**Subscriptions**

are agreements to receive, participate in or access mailing lists and newsgroups.

**Threat**

is any potential event or act, deliberate or accidental, which could cause injury to employees or assets.

**User account**

includes all files, folders, e-mail messages or records of accesses to the Internet contained in an account assigned to a user or in a shared drive.

**Value**

is estimated worth monetary, cultural, intellectual or other.

**Vulnerability**

is an inadequacy related to security that could permit a threat to cause injury.

**Violence**

includes material where physically injurious or violent acts or treatment are being depicted.

**Virus**

is a program that infects a computer by attaching itself to another program and propagating itself when that program is executed.

1 Receipt of unsolicited e-mail that is considered inappropriate as defined in this directive and Sections 10 and 11 in the Policy on the Use of Electronic Resources, must be reported to your supervisor.

2 The standard network (system) refers to the CBSA network that is certified up to and including Protected B information.

3 Only CBSA approved encryption mechanism is to be used.

4 Refer to footnote #1 regarding unsolicited e-mail under Section 5, Context



5 The standard network (system) refers to the CBSA network that is certified up to and including Protected B information.

6 Refer to Chapter 15, Reporting of Security Incidents. Note: Security incidents not involving employee misconduct must be reported as stipulated in this directive.

7 Normal routine analysis refers to monitoring for operational purposes as defined under Section 13 of the Policy on the Use of Electronic Resources.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive sur l'utilisation appropriée du courrier électronique (courriel)

PROTECTION • SERVICE • INTÉGRITÉ





# 1. Date d'entrée en vigueur

Cette directive entre en vigueur dès sa diffusion.

Cette directive, anciennement une politique, remplace la version 1.1 (04 janvier 2010) et intègre des mises à jour administratives à compter du 13 mai 2013.

# 2. Directive

La directive de l'Agence des services frontaliers du Canada (ASFC) sur l'utilisation appropriée du courrier électronique (courriel) est fondée sur la Politique de l'ASFC sur l'utilisation des ressources électroniques. La présente directive développe et explique les exigences en matière de sécurité touchant l'utilisation appropriée du courriel dont fait mention la Politique sur l'utilisation des ressources électroniques de l'ASFC.

# 3. Objectif de la directive

La présente directive a pour objectif de s'assurer que les personnes autorisées de l'ASFC utilisent le courriel de l'ASFC de façon appropriée conformément aux lois, aux politiques, aux normes et aux lignes directrices du gouvernement du Canada ainsi qu'aux politiques, aux normes et aux lignes directrices de l'ASFC.

La directive vise également à informer les utilisateurs autorisés de l'ASFC de leurs obligations et de leurs responsabilités quant à l'utilisation appropriée et autorisée du système de courriel de l'ASFC.

# 4. Portée et application

La présente directive s'applique à :

1. tous les services de courriel offerts par l'ASFC;
2. toutes les personnes autorisées qui ont accès au courriel de l'ASFC.

La directive exige que toutes les personnes autorisées lisent et comprennent la Politique sur l'utilisation des ressources électroniques de l'ASFC.







## 5. Contexte

L'ASFC utilise le courriel comme un outil de communication essentiel dans le cadre des activités et des opérations quotidiennes de l'Agence. Les personnes autorisées doivent utiliser cet outil de façon responsable, efficace et légale pour promouvoir et appuyer le mandat de l'ASFC.

Les utilisateurs du système de courriel doivent savoir qu'ils sont responsables de tous les messages électroniques qu'ils créent, envoient ou reçoivent[1] à l'aide du courriel de l'ASFC.

Les courriels sont conservés sur du matériel informatique de l'ASFC, même une fois que l'auteur ou le destinataire a supprimé le message. Une fois que le courriel a quitté le coupe-feu, les passerelles ou les systèmes de l'Agence du revenu du Canada (ARC) ou des Services partagés Canada (SPC), il n'est plus protégé contre une interception ou une modification s'il n'est pas chiffré. Les messages organisationnels créés, reçus ou distribués par le courriel de l'ASFC sont la propriété de l'Agence des services frontaliers du Canada et doivent être gérés comme une ressource d'information du gouvernement.

## 6. Définitions

**Accès**

L'entrée en communication avec les ressources de courriel offertes par l'ASFC aux personnes autorisées ou l'utilisation de ces ressources. L'accès à de telles ressources peut se faire tant à l'intérieur qu'à l'extérieur des installations du gouvernement. Cet accès permet le télétravail et l'utilisation à distance et peut également s'appliquer à des personnes autorisées qui utilisent les ressources de courriel fournies par l'ASFC à des fins personnelles limitées, en dehors des heures de travail, conformément à la présente directive et à la politique sur l'utilisation des ressources électroniques de l'ASFC.

**Personnes autorisées**

Comprennent les employés de l'ASFC, les entrepreneurs et d'autres personnes qui sont autorisés par la direction à avoir accès aux ressources électroniques de l'ASFC et à son service de courriel.

**Courrier électronique (courriel)**

Comprend tous les messages et transmissions électroniques créés, stockés, reçus et distribués à l'aide du système de courriel de l'ASFC, y inclus les dispositifs portables et sans fil. Les services et les systèmes de courriel de l'ASFC comprennent le système et les services de l'Agence, l'internet, d'autres services de courriel internes autorisés de l'ASFC ainsi que les réseaux publics et privés indépendants de l'Agence. Le courriel, aux fins de la présente










directive, comprend toujours les services d'infrastructure et de courriel que l'ARC et le SPC offre à l'ASFC.

**Surveillance du courriel** Désigne les mesures consistant à enregistrer puis à analyser les activités ou l'utilisation des services définis dans la politique sur l'utilisation des ressources électroniques de l'ASFC. Les renseignements enregistrés aux fins d'analyse ne comprennent pas d'habitude le contenu des messages électroniques, des fichiers et des transmissions.

Pour obtenir d'autres définitions, vous pouvez consulter l'annexe « C » du présent document ou le lexique de la DGIST (Entrez la sécurité informatique pour obtenir que les définitions de la sécurité informatique).

## 7. Énoncé de la directive

L'Agence des services frontaliers du Canada a pour politique de donner aux personnes autorisées l'accès aux services de courriel approuvés par l'Agence pour mener les affaires du gouvernement. Ceci peut comprendre communiquer avec des employés de la fonction publique et le public, recueillir des renseignements reliés à leurs fonctions, selon le besoin d'en connaître, et développer des compétences sur l'utilisation de ces ressources.

Les services de courriel offerts à l'ASFC et fournis par celle-ci sont réservés aux activités de l'Agence. L'utilisation personnelle à des fins limitées est autorisée à condition de respecter la Politique sur l'utilisation des ressources électroniques de l'ASFC de même que les autres politiques et dispositions législatives relevant de l'ASFC ainsi que des gouvernements fédéraux et provinciaux. Les services de courriel font l'objet d'une surveillance et sont assujettis aux exigences et aux demandes liées à l'Accès à l'information et à la protection des renseignements personnels (AIPRP).

## 8. Exigences de la directive

Toutes les lois régissant les communications écrites s'appliquent aux services de courriel de l'ASFC, y compris la *Loi sur l'accès à l'information*, la *Loi sur la protection des renseignements personnels*, la *Loi sur la Bibliothèque et les Archives du Canada*, la *Loi sur les langues officielles*, la *Loi canadienne sur les droits de la personne*, le *Code criminel* et le *Code de valeurs et d'éthique de la fonction publique*.

En vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, les personnes peuvent avoir accès aux fichiers électroniques, sous réserve des exemptions applicables selon ces lois.







# 9. Utilisation acceptable du courriel

Les services de courriel doivent servir aux activités officielles afin de réaliser le mandat et la mission de l'ASFC. Seuls les services et les systèmes de courriel approuvés et appuyés par l'ASFC doivent être utilisés, y compris tout dispositif ayant une capacité de service de messagerie électronique. Aucun autre fournisseur ou système (p.ex. Hotmail, GMail, Yahoo mail ou le fournisseur de service personnel de l'utilisateur) ne peut être utilisé. Les personnes autorisées qui utilisent les services de courriel de l'ASFC doivent respecter les interdictions visant des activités criminelles, illicites ou inacceptables énoncées dans la Politique sur l'utilisation des ressources électroniques de l'ASFC et la présente directive. Elles doivent également respecter toutes les dispositions législatives, les politiques et les lignes directrices pertinentes.

Les services de courriel de l'ASFC doivent être utilisés à des fins approuvées, notamment :

1. La réalisation d'activités gouvernementales telles que :
   - communiquer et partager de l'information avec des collègues, d'autres ministères et le secteur privé pour l'exécution des fonctions et des activités de l'ASFC;
   - recueillir des renseignements reliés aux fonctions de l'utilisateur;
   - annoncer des événements de groupe qui sont autorisés et appuyés par la direction de l'ASFC, p. ex. des collecte de fonds pour une campagne de charité;
   - utiliser les listes de distribution pour transmettre de l'information à des fins officielles;
   - mener des activités de perfectionnement professionnel liées aux fonctions du poste.
2. L'utilisation personnelle à des fins limitées (durant les pauses-repas, les périodes de repos ou après le travail et entreprendre des activités, tel que spécifié dans le Code de conduite de l'ASFC), telle que :
   - communiquer avec des parents, des amis, et d'autres personnes à des fins non officielles;
   - accéder à des nouvelles acceptables et autres sources d'information qui ne sont pas prohibées ou restreintes en vertu d'une loi ou d'une politique;
   - exécuter des transactions bancaires personnelles de routine;
   - exécuter une activité syndicale qui est expressément autorisée au préalable par le gestionnaire compétent.
3. Toute autre fin qui est conforme à la Politique d'utilisation des réseaux électroniques du Conseil du Trésor, la Politique sur l'utilisation des ressources électroniques de l'ASFC et la présente directive ou qui est expressément autorisée par écrit par la direction.

L'utilisation du courriel pour des activités comme des événements spéciaux et des listes de distribution doit être approuvée au préalable par la direction.





Agence des services frontaliers du Canada | Canada Border Services Agency



## Conditions de l'utilisation personnelle à des fins limitées

L'utilisation personnelle à des fins limitées des systèmes de courriel est permise à la condition de respecter toutes les dispositions législatives et les politiques pertinentes de l'ASFC et des gouvernements fédéraux et provinciaux.

L'utilisation personnelle à des fins limitées du courriel de l'ASFC par les personnes autorisées ne doit pas :

1. Nuire à la productivité ou à l'exécution des fonctions officielles de l'utilisateur.
2. Entraîner des coûts directs pour l'Agence.
3. Faciliter une activité criminelle, illicite ou inacceptable définie dans la Politique sur l'utilisation des ressources électroniques de l'ASFC.
4. Constituer un fardeau à l'égard du rendement ou de la capacité de stockage des ressources électroniques de l'ASFC.

## Utilisation du courriel à des fins syndicales

Il faut obtenir au préalable l'approbation des Relations de travail de l'ASFC afin d'utiliser le courriel pour transmettre des avis syndicaux ou autre documentation syndicale.

Le courriel à des fins syndicales :

1. Peut être utilisé pour communiquer avec la direction, les Ressources humaines, les Relations de travail et le Système de gestion informelle des conflits (SGIC).
2. Ne peut pas être utilisé pour des communications générales avec les membres du syndicat, à moins d'obtenir une autorisation explicite auprès de la direction.
3. Peut être utilisé par des représentants syndicaux pour communiquer avec un employé afin de répondre à une demande personnelle tel qu'un grief ou une autre question patronale / syndicale.
4. Doit être en conformité avec le droit de l'employé à la protection des renseignements personnels et l'ASFC ne devrait pas considérer le contenu de tels courriels comme étant contraire aux intérêts de l'Agence ou de ses représentants.

Les représentants syndicaux sont responsables des messages électroniques qu'ils produisent ou diffusent à partir de leur compte de l'ASFC.

## Protection des communications par courriel

Les courriels envoyés à l'extérieur du réseau du gouvernement du Canada ne sont pas protégés. Par conséquent, les utilisateurs doivent faire attention au contenu des messages qu'ils envoient à l'extérieur du système de courriel du gouvernement.







Les communications par courriel doivent être protégées de la façon décrite ci-dessous lorsqu'elles sont transmises par le réseau standard2 de l'ASFC / ARC, à un destinataire identifié d'un ministère ou d'un organisme fédéral ou à l'extérieur de l'agence.

1. Les renseignements non classifiés peuvent être transmis sans autre mesure de contrôle comme le chiffrement.3
2. Les renseignements protégés A peuvent être transmis sans autre mesure de contrôle comme le chiffrement, sauf lorsqu'une évaluation de la menace et du risque (EMR) recommande le chiffrement des renseignements au niveau protégé A.
3. Tous les renseignements protégés B doivent être chiffrés.
4. Les renseignements protégés C ou classifiés ne doivent pas être transmis par le système de courriel standard.

## Renseignements organisationnels et transitoires (temporaires)

Tous les courriels, y compris les pièces jointes, qui sont créés, reçus ou transmis dans le cours normal des activités de l'ASFC et qui contiennent des renseignements sur les fonctions, les activités et les décisions de l'ASFC doivent être conservés. Tous les utilisateurs sont donc responsables de la gestion efficace des courriels qu'ils créent ou reçoivent dans leur boîte aux lettres électronique. Les courriels sont considérés comme étant des documents officiels de l'ASFC. Ils doivent être conservés et protégés contre une destruction ou un accès non autorisé. Voir l'annexe « A » de la présente directive portant sur les renseignements organisationnels et transitoires. Consultez la Politique de l'ASFC sur le programme de gestion de l'information et la politique du Secrétariat du Conseil du Trésor sur la gestion de l'information gouvernementale (GIG) pour obtenir de plus amples renseignements.

## Autres considérations

Le courriel ne doit pas être utilisé pour créer, stocker, transmettre ou solliciter4 des messages inappropriés, illicites ou inacceptables tels que des chaînes de lettres, des blagues, de la pornographie, etc.

Les communications impliquant l'utilisation des ressources électroniques, y compris l'utilisation de l'internet, seront surveillées.

Les messages électroniques ne doivent pas être incendiaires, malveillants, diffamatoires ou perturbateurs pour le gouvernement du Canada, l'ASFC, les partenaires externes, les organisations ou les personnes.

Toute information, y inclus les courriels, doivent être désignés et classés de manière appropriée conformément à la politique de sécurité de l'ASFC, Chapitre 5, Désignation des renseignements et des biens classifiés et protégés.

Les courriels non sollicités, aussi connus comme les pourriels, doivent être supprimés sauf si le pourriel inclut du matériel extrêmement offensant, illicite ou criminel.







Des renseignements supplémentaires concernant le courriel, tel que les comptes extérieurs à l'Agence, les renvois automatiques, le courriel sans fil et les comptes génériques, sont disponibles dans les politiques de sécurité suivantes : Chapitre 17, Responsabilité et authentification de l'accès aux systèmes des technologies de l'information de l'Agence et le Chapitre 23, Sécurité des communications (COMSEC).

Voir l'annexe B pour obtenir des renseignements supplémentaires sur les pourriels.

## 10. Activités criminelles, illicites ou inacceptables

L'utilisation du courriel ne doit pas servir à des activités criminelles, illicites ou inacceptables telles que décrites dans la Politique sur l'utilisation des ressources électroniques de l'Agence et toute autre politique applicable.

On trouvera des exemples de ce genre d'activités aux annexes A, B et C de la Politique sur l'utilisation des ressources électroniques de l'ASFC.

## 11. Rôles et responsabilités

### Personnes autorisées

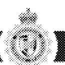
Les personnes autorisées qui ont accès au courriel de l'ASFC doivent respecter la présente directive, toutes les politiques et les lois du gouvernement et sont responsables des activités qu'elles mènent en utilisant les services du courriel de l'ASFC.

Les personnes autorisées qui utilisent le courriel de l'ASFC doivent :

1. S'assurer d'utiliser le courriel de l'ASFC à des fins gouvernementales et à des fins autorisées par la direction.
2. Gérer les messages électroniques en conformité avec les lignes directrices sur la gestion des documents de l'ASFC.
3. Déclarer immédiatement la réception d'un courriel qui n'observe pas la directive à leur superviseur, qui veillera à assurer un suivi au niveau approprié.
4. Chiffrer toutes les communications contenant des renseignements délicats protégés B (tel que détaillé dans la présente directive sous la section Protection des communications par courriel).
5. Signer numériquement, au besoin, les renseignements de nature délicate Protégé A ou B afin d'authentifier les messages électroniques.[5]
6. En aucun cas transmettre des renseignements protégés C ou classifiés par courriel.







## Gestionnaires

Les gestionnaires doivent s'assurer que les utilisateurs sont au courant de la directive sur le courriel. De plus, ils doivent s'assurer que les utilisateurs ont lu et compris la Politique sur l'utilisation des ressources électroniques de l'ASFC.

Les gestionnaires doivent signaler les cas d'utilisation criminelle, illicite ou inacceptable soupçonnée du courriel de l'ASFC au directeur, Sécurité des TI ou à la Direction de la sécurité et des normes professionnelles.[6]

## Agent de sécurité du ministère (ASM)

L'Agent de sécurité du ministère se réserve le droit d'accorder l'accès au courriel d'un utilisateur dans le cadre d'une enquête officielle ou pour répondre aux exigences opérationnelles de l'Agence. Une approbation écrite doit être fournie et la procédure sur la façon dont on a eu accès aux renseignements doit être notée.

L'agent de sécurité du ministère est tenu de :

1. Renvoyer les gestionnaires à la Direction de la sécurité et des normes professionnelles pour les demandes d'accès aux courriels ou aux fichiers se trouvant dans le compte d'un utilisateur
2. Renvoyer les gestionnaires à la Direction de la sécurité et des normes professionnelles lorsqu'on soupçonne un mauvais usage des ressources électroniques de l'Agence.
3. Mener une enquête sur les rapports d'utilisation criminelle, illicite ou inacceptable des services de courriel de l'ASFC.
4. Demander conseil aux Relations de travail et aux Services juridiques sur les cas présumés d'utilisation criminelle ou illicite des services de courriel de l'ASFC et sur le signalement aux autorités chargées de l'application de la loi, s'il y a lieu.
5. Répondre à toute demande relative à la Loi sur l'accès à l'information qui se rapporte à l'application de cette directive.

## Relations de travail

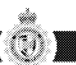
Les Relations de travail peuvent offrir des conseils à la Sécurité des TI et la Direction de la sécurité et des normes professionnelles à l'appui d'une enquête sur l'utilisation illicite ou inacceptable du courriel.

# 12. Vie privée et surveillance

## Attentes quant au respect de la vie privée







La Charte canadienne des droits et libertés garantit que les personnes autorisées du gouvernement ont le droit de s'attendre raisonnablement au respect de la vie privée, y compris au travail.

Les copies des fichiers et des courriels (y compris les documents supprimés) sont sauvegardées automatiquement et conservées quotidiennement. Leur contenu peut être consulté en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, sous réserve des exemptions qui y sont prévues.

### Surveillance du courriel

La Direction de la sécurité et des normes professionnelles (DSNP) est l'autorité fonctionnelle responsable de la surveillance du contenu. La surveillance peut s'appliquer, sans s'y limiter, à la consultation du contenu et à l'analyse du volume de fichiers, de courriels ou de registres dans les cas où l'on soupçonne une utilisation abusive.

Si, par suite d'une analyse ordinaire[7] ou d'une plainte, il y a un motif de soupçonner qu'une personne fait une utilisation abusive des ressources électroniques de l'Agence, la question est renvoyée à la DSNP pour enquête. Celle-ci peut autoriser la surveillance sans préavis, y compris la lecture ou l'examen du contenu des courriels ou des fichiers de l'intéressé.

Une surveillance au hasard peut être menée conformément à la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels* et le *Code criminel*.

## 13. Mesures disciplinaires

Les personnes qui ne respectent pas la présente directive peuvent faire l'objet de mesures disciplinaires pouvant aller jusqu'au congédiement, telle qu'énoncées dans la Politique sur l'utilisation des ressources électroniques de l'ASFC.

## 14. Examen de la directive

La présente directive sera revue au moins tous les cinq ans sous la direction du directeur général, Services d`infrastructure, du directeur général, Direction de la sécurité et des normes professionnelles et de l'agent de sécurité du ministère (ASM).

## 15. Références

### Lois et politiques pertinentes





- Code de conduite de l' ASFC
- Code de valeur et d'éthique de la fonction publique
- Politique de l'ASFC en matière de discipline et Lignes directrices en matière de discipline
- Politique de l'ASFC sur la sécurité des communications (COMSEC)
- Politique sur l'utilisation des ressources électroniques de l'ASFC
- Lignes directrices concernant la politique sur l'utilisation des ressources électroniques de l'ASFC
- Les politiques de sécurité de l'ASFC
- Gestion du courrier électronique - Politique de l'ASFC
- Gestion du courrier électronique - Lignes directrices et procédures de l'ASFC
- *Loi sur la gestion des finances publiques*
- *Loi sur l'accès à l'Information*
- *Loi sur la protection des renseignements personnels*
- *Charte des droits et libertés*
- *Loi sur la Bibliothèque et les Archives du Canada*
- *Loi sur la protection de l'information*
- *Code criminel*
- *Loi sur la responsabilité civile de l'État et le contentieux administratif*
- *Loi sur le droit d'auteur*
- *Loi sur les marques de commerce*
- *Loi canadienne sur les droits de la personne*
- *Loi sur les langues officielles*

## Renvois

Politiques et publications du Conseil du Trésor

- Politique sur le harcèlement en milieu de travail
- Politique sur la sécurité du gouvernement
- Politique de communications du gouvernement du Canada
- Guide d'Internet du Gouvernement du Canada
- Politique sur la gestion de l'information gouvernementale (GIG)
- Gestion de la sécurité des technologies de l'information (GSTI)
- Directive sur les pertes de fonds et de biens
- Politique sur la protection des renseignements personnels
- Politique d'utilisation des réseaux électroniques du SCT
- Politique sur le télétravail
- Lignes directrices concernant la discipline du SCT

# 16. Demandes de renseignements

Les demandes de renseignements concernant la présente directive doivent être adressées aux responsables suivants :



Direction générale de l'information, des sciences et de la technologie
Sécurité et continuité de la TI
Courriel : Sécurité et continuité de la TI

Direction générale du contrôle
Direction de la sécurité et des normes professionnelles
Courriel : Direction de la sécurité et des normes professionnelles

## Annexe A — Renseignements organisationnels et transitoires

Tous les utilisateurs autorisés qui créent, reçoivent, utilisent ou transmettent des renseignements à l'aide du courriel de l'ASFC doivent respecter les lignes directrices suivantes.

Renseignement organisationnel — information enregistrée sous diverses formes, y compris des données dans des systèmes informatiques; des documents électroniques ou sur papier comme de la correspondance, des notes de service, des plans, des cartes et des dessins; des enregistrements sonores; des courriels; des images électroniques et tout autre matériel documentaire créés et reçus par une organisation ou une personne pour exécuter des fonctions officielles.

- Messages qui reflètent la position ou les activités de l'ASFC.
- Messages qui amorcent, autorisent ou terminent une transaction commerciale.
- Messages reçus de sources externes qui sont clairement dans l'intérêt de l'ASFC pour exécution de ses activités.
- Ébauches de courriels montrant l'évolution d'un document tout au long du processus d'approbation.
- Copies contenant plus ou moins d'information que le document original.
- Messages originaux sur des politiques ou des directives.
- Messages originaux du maître de poste.

Si l'information n'existe pas ailleurs :

Messages reliés aux horaires de travail et à l'affectation du personnel.
Ordre du jour et procès-verbaux des réunions; notes d'information.
Rapports finaux et recommandations.

## Un courriel identifié comme étant de l'information organisationnelle doit être conservé

Renseignement transitoire — information qui est requise uniquement pour un temps limité pour s'assurer qu'une activité de routine est exécutée ou qu'un document subséquent est préparé. L'information transitoire ne comprend pas l'information requise par les institutions





gouvernementales ou les ministres pour contrôler, appuyer ou documenter la prestation des programmes, exécuter des opérations, prendre des décisions ou rendre compte des activités.

## Un courriel comportant de l'information transitoire devrait être supprimé lorsqu'il n'est plus utile, par exemple :

- Les messages qui sont des copies de l'information utilisée à des fins de références et non des documents officiels.
- Les messages utilisés pour une simple communication.
- Les messages informels ou les ébauches qui ne constituent pas une preuve dans l'élaboration d'un document; les messages qui sont des copies de l'information.
- Les divers avis de réunions du personnel, de vacances, etc.
- Les messages provenant d'une liste de distribution ou autres sources internet, uniquement à des fins de référence.
- Des copies utilisées à des fins d'information ou de référence uniquement lorsque des renseignements supplémentaires ont été incorporés dans des versions subséquentes.
- Les brouillons ou les ébauches qui ne sont pas requises pour documenter l'évolution d'un document.
- L'information non reliée aux activités de l'ASFC, par exemple les annonces ou les annonces publicitaires non sollicitées provenant de sources externes.

Note : Vous ne devez pas supprimer les courriels contenant de l'information transitoire après avoir reçu une demande officielle en vertu de la *Loi sur l'accès à l'information* ou *la Loi sur la protection des renseignements personnels* reliée à cette information. Au moment d'une telle demande, toute l'information existante doit être prise en considération en vue d'une communication possible, qu'elle soit transitoire ou non. La liste ci-dessus donne des exemples; il ne s'agit pas d'une liste exhaustive de l'information que vous devez conserver.

## Annexe B — Pourriels

Les pourriels sont des courriels non désirés et non sollicités provenant d'une adresse externe. La plupart des pourriels sont des annonces publicitaires et devraient être supprimés. Cependant, certains pourriels peuvent inclure du matériel extrêmement offensant, illicite ou criminel, par exemple de la pornographie juvénile ou des escroqueries, et doivent donc être signalés.

Exemples de pourriels qui doivent être supprimés :

Annonces publicitaires pour des pilules, des logiciels, des bijoux, des fournitures, des cours ou de la formation, des services de rencontre et des alertes pour des actions ou des investissements.
Messages demandant ou offrant un emploi.

Exemples de pourriels à signaler :

Messages contenant des images de pornographie juvénile, des annonces publicitaires ou des liens à cet effet.



Demandes de renseignements personnels, par exemple des numéros de carte de crédit, un nom d'utilisateur et un mot de passe pour des services bancaires en ligne (pêche aux données personnelles – hameçonnage).
Messages contenant du matériel pornographique.
Messages impliquant des opérations pyramidales.

Si un pourriel est considéré comme étant un incident de sécurité, communiquez avec votre support local de la TI et la Direction de la sécurité et des normes professionnelles de la Direction générale du contrôle.

## Annexe C — Termes et définitions

La présente annexe présente une liste alphabétique des termes et des explications que comportent la présente directive et la Politique sur l'utilisation des ressources électroniques de l'ASFC. Il s'agit d'un guide de référence pour aider les utilisateurs à mieux comprendre les dispositions de ces politiques.

**Abonnements**
ententes pour recevoir, participer ou accéder à des listes de distribution et des groupes de nouvelles.

**Activité privée**
une activité menée en dehors du travail pour en tirer un profit personnel, y compris la vente ou l'achat de biens et de services. Cette catégorie comprend aussi la conduite d'activités politiques

**Administration du contenu**
peut comprendre, entre autres, l'installation des messages à l'extérieur du bureau ou l'extraction de documents organisationnels.

**Biens**
Éléments d'actifs corporels ou incorporels du gouvernement du Canada. Ce terme s'applique, sans toutefois se limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale.

**Chaîne de lettres**
courriels n'ayant qu'un seul but - vous inciter à les transmettre à d'autres. Ils offrent faussement de la chance, de l'argent ou un souhait lorsqu'ils sont transmis.

**Compromission**
comprend un préjudice causé par la divulgation non autorisée, la destruction, le retrait, la modification, l'interruption ou l'utilisation des biens.

**Compte d'utilisateur**



comprend tous les fichiers, dossiers, courriels ou documents d'accès à internet contenus dans le compte attribué à un utilisateur ou dans une unité partagée.

**Confidentialité**

Il s'agit de la caractéristique selon laquelle les renseignements ne doivent pas être divulgués à des personnes non autorisées, car cela pourrait porter préjudice à l'intérêt national ou à d'autres intérêts, comme l'indiquent les dispositions précises de la Loi sur l'accès à l'information, de la Loi sur la protection des renseignements personnels.

**Contenu à caractère sexuel**

matériel ne comportant pas d'acte sexuel explicite (détaillé), mais dont visant à provoquer une excitation sexuelle ou une titillation. Il est évident qu'un thème sexuel pour adulte est présenté ou décrit.

**Disponibilité**

La condition d'être disponible sur demande afin de soutenir les opérations, les programmes et les services.

**Documents**

renseignements présentés dans un format physique ou électronique, y compris un document audio-visuel, une photographie, une carte, un dessin, un film, un enregistrement sonore, un enregistrement magnétoscopique, une microforme, une bande magnétique, un document ou un fichier électronique et du matériel documentaire.

**Hameçonnage**

(Phishing) voir Pêche aux données personnelles.

**Incident de sécurité**

comprend un bien, une loi ou une omission qui pourrait entraîner une compromission, une menace ou un acte de violence envers les employés.

**Intégrité**

exactitude et intégralité des biens et authenticité des transactions.

**Jeu**

miser, parier ou risquer de l'argent ou un bien de valeur sur un jeu de hasard ou un mélange de compétence et de chance. Le jeu se traduit de diverses façons, y compris les paris sportifs et autres types de paris.

**Jurons**

comprennent le matériel utilisant un langage vulgaire (offensant), y compris, entre autres, un langage vulgaire dans un texte, l'utilisation de mots dans un fichier sonore ou vidéo et même le sous-titre d'une image.

**Matériel offensant**

susceptible d'insulter, de dégoûter ou de répugner. Comprend les blagues concernant certains groupes (p.ex. blagues racistes, sexistes ou à caractère religieux). Peut comprendre des images offensantes (c.-à-d. images de cadavres, de défécation).

**Mauvais usage**







signifie toute action ou inaction d'un utilisateur représentant une activité inacceptable, illicite ou criminelle.

**Menace**

événement ou acte potentiel, délibérée ou accidentel, qui pourrait causer un préjudice aux employés ou aux biens.

**Nudité**

une personne nue ou exhibant ses organes génitaux. N'a pas nécessairement un contenu sexuel.

**Opérations pyramidales**

hiérarchies vous incitant à envoyer de l'argent en espérant qu'un certain nombre de personnes vous enverra ensuite de l'argent.

**Pêche aux données personnelles (hameçonnage)**

forme de fraude sur internet dans laquelle un faux courriel, un faux site Web ou une fausse information, qui semble toutefois authentique, est transmis afin de voler de précieux renseignements tels que les numéros de cartes de crédit, les numéros d'assurance sociale, les noms d'utilisateur et les mots de passe.

**Pornographie**

matériel sexuel explicite conçu pour provoquer une excitation sexuelle ou une titillation.

**Pourriel**

message électronique non désiré et non sollicité provenant d'une adresse externe. La plupart des pourriels sont des annonces publicitaires, mais certains pourraient inclure du matériel criminel, par exemple de la pornographie juvénile ou une fraude.

**Renseignement**

un bien ou une ressource qui est défini comme une donnée, un fait ou une connaissance et qui est consigné, quel que soit la forme, la technologie ou le support d'enregistrement utilisé.

**Renseignements classifiés**

renseignements reliés à l'intérêt national qui peuvent être admissibles à une exemption ou à une exclusion en vertu de la Loi sur l'accès à l'information ou la Loi sur la protection des renseignements personnels, et dont la compromission pourrait raisonnablement causer un préjudice à l'intérêt national. Voir aussi Renseignements délicats.

**Renseignements délicats**

renseignements qui doivent faire l'objet de mesures de protection appropriée en raison de son caractère confidentiel. Voir aussi Renseignement classifié et Renseignement protégé.

**Renseignements protégés**

renseignements reliés à d'autres raisons que l'intérêt national qui peuvent être admissibles à une exemption ou à une exclusion en vertu de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*, et dont la compromission pourrait raisonnablement causer un préjudice à un intérêt non national. Voir aussi Renseignements délicats.

**Ressources électroniques**

Groupes d'ordinateurs, réseaux et systèmes informatiques, fonctions ou dispositifs assignés aux utilisateurs ou aux





programmes. Sans limiter les considérations qui précèdent, ces ressources comprennent l'internet, les fonctions, logiciels et dispositifs internes de l'ASFC ainsi que les fonctions ou dispositifs publics et privés indépendants de l'Agence. Cela comprend aussi le matériel tel que les ordinateurs personnels ou portables, les périphériques, les dispositifs de stockage, les dispositifs sans fil et les supports servant à obtenir, à stocker et à diffuser l'information, etc. De nombreux dispositifs non informatiques, par exemple les caméras numériques et les téléphones cellulaires, sont considérés comme étant des ressources électroniques en vertu de la politique compte tenu de leur capacité de stocker et de distribuer de l'information. Les ressources électroniques, aux fins de la présente directive, comprennent toujours les services d'infrastructure et de réseau que l'Agence du revenu du Canada (ARC) offre à l'ASFC et les services de réseau entre l'ASFC et d'autres organisations gouvernementales.

**Risque**

la chance qu'un point faible soit exploité ou cause un préjudice.

**Salon de clavardage**

sont des groupes de discussion électroniques où les participants peuvent discuter en ligne en temps réel, normalement grâce à l'échange de messages en temps réel.

**Sécurité de la technologie de l'information**

implique des mesures pour protéger la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements stockés, traités ou transmis par voie électronique.

**Surveillance du contenu**

peut s'appliquer, sans s'y limiter, à la consultation du contenu et à l'analyse du volume de fichiers, de courriels ou de registres pour établir s'il y a eu un mauvais usage.

**Systèmes primaires**

bases de données telles les SAE, les applications sur ordinateur central et les applications réseaux. Ils sont fournis uniquement pour exécuter les activités de l'Agence.

**Systèmes secondaires**

comprennent des applications telles le courriel, Microsoft Office et l'internet (lorsqu'une utilisation personnelle limitée est permise).

**Valeur**

la valeur estimée; qu'elle soit monétaire, culturelle, intellectuelle ou autre.

**Violence**

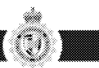
comprend le matériel comportant des actes ou des traitements violents ou injurieux.

**Virus**

programme qui infecte un ordinateur en s'annexant à un autre programme et se propageant lorsque le programme en question est exécuté.

**Vulnérabilité**

faiblesse quant à la sécurité qui pourrait permettre à une menace de causer un préjudice.



1 Veuillez signaler à votre surveillant la réception d'un courriel non sollicité considéré inacceptable tel que défini dans cette directive et les sections 10 et 11 de la Politique sur l'utilisation des ressources électroniques.

2 Le réseau (système) standard de l'ASFC fait référence à celui certifié pour traiter les renseignements jusqu'à et incluant Protégé B.

3 Seule la méthode de chiffrement approuvée par l'ASFC doit être utilisée.

4 Veuillez-vous référer à la note de bas de page #1, sous la Section 5, Contexte, concernant le courriel non sollicité.

5 Seule la méthode de signature numérique approuvée par l'ASFC doit être utilisée.

6 Veuillez-vous référer au Chapitre 15, Signalement des incidents de sécurité. Note : Tous les incidents de sécurité doivent être signalés selon cette directive à l'exception des incidents concernant l'inconduite d'un employé.

7 Une analyse ordinaire fait référence à la surveillance pour des motifs opérationnels telle que précisée sous la Section 13 de la Politique sur l'utilisation des ressources électroniques.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Guidelines for the Directive on the Appropriate Use of E-mail

PROTECTION • SERVICE • INTEGRITY

Canada



# 1. Introduction

The Directive on the Appropriate Use of Electronic Mail (e-mail) summarizes users' obligations and responsibilities for the appropriate use of CBSA's e-mail system.

E-mail services provided for and by CBSA are for business purposes. Limited personal use is permitted if it complies with CBSA's Policy on the Use of Electronic Resources as well as all other applicable CBSA, federal and provincial policies and legislation. E-mail services are subject to monitoring and Access to Information and Privacy (ATIP) requirements and requests.

These guidelines, based on the directive on the Appropriate Use of e-mail are intended to provide guidance about the responsible use of the CBSA e-mail systems and services. The guidelines outline key responsibilities as a user of CBSA's e-mail system and provide concrete examples of how the e-mail directive applies to everyday use.

# 2. CBSA E-mail

CBSA e-mail is intended for corporate use. You need to be conscientious when sending e-mail. E-mail remains stored on CBSA systems, even after the originator or recipient has deleted the message. Also, once e-mail is sent outside the control of CBSA systems, such as via the Internet, it can be intercepted or altered, unless encrypted. An email message sent outside of the Agency is like a postcard: anyone can read it therefore as a user you should not have an expectation of privacy.

When sending or receiving e-mail:

- Think, write, read, and edit before sending e-mail.
- Be sure that each person on a distribution list has a "need-to-know" of the e-mail message content or attached documents.
- If the message contains sensitive information, there may be a need to encrypt it (see below for details regarding encryption).

How we use the e-mail services, what we use it for, and even when we use it are all things for us to consider in our day-to-day work. Please take a few moments to learn what you can do to help all of us make best use of this important corporate resource.

# 3. E-mail Responsibilities



E-mail has become a fast and efficient means of communication for users in the Canada Border Services Agency (CBSA). It is used as a business communication tool that is critical to the daily operations and business of the Agency. The information you collect or create while conducting business is the property of CBSA. Therefore, you have to consider the Agency's business, legislative, and accountability requirements when you manage the content of e-mail messages, just as you would with paper or other non-electronic information.

When using e-mail on a daily basis to perform your work, you have a responsibility to protect CBSA's information and assets. The following is a summary of your responsibilities. Please refer to the Directive on the Appropriate Use of E-mail for further details.

- Do not send sensitive information such as client and employee information using the standard CBSA e-mail systems because they are not secure. There are potential risks that sensitive information could be read by, or misdirected to, unauthorized persons and destinations if such information is transmitted electronically without the proper controls and safeguards.
- Do not engage in activities that are criminal, unlawful, or unacceptable. You can find some examples of these activities in the Policy on the Use of Electronic Resources and in the CBSA Code of Conduct.
- Learn how to manage and protect e-mail as there are certain risks associated with using e-mail.
- Report any criminal or unlawful breach of computer security, policies, and standards to your supervisor.
- Be informed of all CBSA and Government of Canada applicable policies, standards and laws.
- Contact your supervisor when in doubt about proper procedures and acceptable uses of the CBSA e-mail services and systems.

## 4. Appropriate Use of the E-mail System

E-mail is a valuable tool but it is not always the best choice for communicating. For example, you would not send a job performance message by e-mail. Instead, you would deliver the message in a private meeting. When you need to communicate information, also consider if it would be more appropriate to use the telephone or send the message by fax.

As e-mail has become widely accessible, an online "etiquette" has evolved.

- Be polite. Common courtesy applies to e-mail as much as it does in face-to-face communication.
- Make sure you are clear and concise.
- The subject line should be descriptive but brief.
- Always specify what action you want from the recipient.



# 5. Authorized Uses of E-mail

The e-mail services are to be used for official business to carry out the mandate and mission of CBSA. Your e-mail use must be restricted to CBSA supported and approved e-mail services and systems including all devices capable of any type of electronic messaging.

CBSA's electronic e-mail services are to be used for approved purposes, such as:

- Communicating and sharing information with colleagues, other government departments and the private sector in the performance of CBSA functions and activities.
- Limited personal use. For example, communicating with family, friends and other persons for other than official purposes or conducting routine personal banking transactions, (during lunch break, periods of rest or after work, and activities, as specified in the CBSA Code of Conduct)

All uses of e-mail services for activities such as special events and distribution lists require prior approval by management. Use of e-mail for union notices or other union material requires prior approval of CBSA Labour Relations.

For further details regarding authorized uses of e-mail, consult the Directive on the Use of Appropriate E-mail.

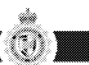
# 6. Unacceptable or Unlawful Uses of E-mail

Only supported and approved CBSA e-mail services and systems are to be used. No other e-mail providers / systems (for example, Hotmail, GMail, Yahoo Mail, a user's personal service provider) are to be used.

You must not use CBSA e-mail to create, store, transmit or solicit inappropriate, unlawful and unacceptable activities such as chain letters, pornography, etc. If you receive unsolicited e-mail that is considered inappropriate as defined in the e-mail directive and Sections 10 and 11 in the Policy on the Use of Electronic Resources, you must report it to your supervisor.

Do not distribute chain letters, games, executable file attachments or large file attachments (for example, pictures). If a large amount of these types of files or documents are sent via the e-mail system, it can overload the services and "crash" the system. It may take significant effort to restore the email service.

For further guidance on and examples of unacceptable use of the CBSA e-mail system, and for direction on security related questions such as sending protected information, consult the Policy on the Use of Electronic Resources and refer to the CBSA Security Policies found under the Comptrollership Manual, Security Volume.



# 7. Monitoring E-mail

CBSA monitoring occurs mainly for operational reasons to determine whether the resources / networks are operating efficiently, to isolate and resolve problems, and to determine if utilization complies with CBSA policies and legislation.

While CBSA's monitoring practices must be conducted in accordance with the *Charter of Rights and Freedom*, the *Privacy Act* and the *Criminal Code*, there are several reasons why you should never assume that your e-mail will remain private. Communication involving use of e-mail resources, including Internet use, will be monitored.

If there are grounds to suspect that an individual is misusing the Agency's electronic resources, the matter will be referred to Corporate Security and Internal Affairs Division (CSIAD) for further investigation. CSIAD is the functional authority for content monitoring. The content monitoring function may include, but is not limited to, viewing the content and analyzing the volume of files, e-mails or logs where there are grounds to suspect misuse.

CSIAD will keep the information confidential and use it only for authorized purposes such when conducting CBSA internal investigations and in accordance with applicable Laws.

Refer to the Directive on the Appropriate Use of E-mail as well as the Policy on the Use of Electronic Resources for more details.

# 8. Types of E-mail

As a user of the CBSA e-mail system, you are responsible for the effective management of all e-mail messages you create, solicit or transmit by means of your e-mail mailbox. E-mail messages are considered official records of CBSA. They must be preserved and protected from unauthorized destruction and access.

E-mail messages are considered either corporate information or transitory information. You must take steps to ensure that corporate information be captured as part of the Agency's corporate memory.

The difference between corporate information and transitory information is as follows:

## 8.1 Corporate information

- is recorded information derived from the actions, transactions, business processes, functions and activities of the CBSA.
- must be retained as part of the corporate memory.





## 8.2 Transitory information

- is information that is required for a limited time to ensure the completion of a routine action or the preparation of a subsequent document.
- can be deleted once the routine action is completed. However, if an Access to Information (ATIP) request has been made, you must retain the information until the request for information has been completed.

## 8.3 Deleted e-mail records

When an e-mail record is deleted, it is generally not permanently destroyed. E-mail records are usually recoverable even when they have been deleted or expunged.

For additional information of corporate and transitory information, consult the Information Management Directive on the Management of E-mail.

# 9. Classification and Labelling of E-mail

## 9.1 Classification of e-mail

Information classification and sensitivity is important for protecting unauthorized disclosure of CBSA's data. The Guidelines on the Use of Electronic Resources provides an overview to help you determine what is considered Protected information (Protected A, B or C) and Classified information (Confidential, Secret or Top Secret).

## 9.2 Labelling of e-mail

The purpose of labelling e-mail containing sensitive information, as with all other forms of information, is to draw the attention of users so that they apply the appropriate safeguards.

If you are the originator of an e-mail, you have the responsibiity of assigning the appropriate security level (in the subject line or first line of text) as Unclassified, Protected A or Protected B.

Also, when there is a concern about the distribution of e-mail beyond the original recipients, as the originator, you should add the caveat "restricted access" (in the subject line or first line of text).

For further details, consult the Security Volume, Chapter 5, Identifying Classified and Protected Information and Assets.



# 10. Protecting Your Information

## 10.1 Protecting sensitive information in an e-mail

Before sending any e-mail or attachment, ensure you ask yourself the following questions:

- What is the classification of the information?
- Where is the message being sent?
- Should it be encrypted?

Refer to section 9 and details of section 10 of these guidelines to assist you in answering these questions. Also, refer to the CBSA Guidelines on the Use of Electronic Resources, the Security Volume, Chapter 5, Identifying Classified and Protected Information and Assets and Chapter 23, Communication Security (COMSEC).

## 10.2 When to encrypt e-mail

E-mail sent outside the Government of Canada network is not secure. Therefore, users should exercise caution about the content of messages they send outside the Government's mail system.

E-mail communications must be protected when they are transmitted across the CBSA / CRA standard network, to an identified recipient of a federal government department or agency, or outside the Agency. Currently, the approved encryption and digital signing tool is Entrust PKI.

1. Unclassified information can be transmitted with no additional controls, such as encryption.
2. Protected A information can be transmitted with no additional controls, such as encryption, except where a Threat and Risk Assessment (TRA) recommends encryption for information at the Protected A level.
3. All Protected B information must be encrypted.
4. Protected C or Classified information must not be transmitted via the standard e-mail system.

WinZip can be used to encrypt e-mail attachments sent to non-government organizations. The same password is used by the originator and the recipient. You should communicate the password by regular (land line) phone. For further information, refer to the WinZip encryption guideline document (pdf, 1624 KB).

For Protected C and above, contact Corporate Security and Internal Affairs Division for advice and guidance: Corporate Security section on Atlas.

For further details on Entrust PKI, please contact your local IT help desk.

## 10.3 E-mail Delegation



You must never share your password to allow someone to access your email account. Good news! You can securely share your account, for business purposes only, by delegating your e-mail access.

MS (Microsoft) Outlook allows you to authorize someone to read, write and / or modify only business related messages from your account during your absence.

The following steps will detail how you can turn on the delegation option and choose the permissions you want to delegate.

- From the MS Outlook Standard Toolbar, click on Tools, Options.
- Click on the Delegates tab.
- Click on Add.
- Select a User Name from the Global Address List, click on Add and click on OK.
- The name will appear in the right hand box Add Users.
- A new box will open.
- Click on the down arrow for the Inbox option to delegate permissions.
- Select one of the options (Reviewer, Author or Editor).
- Click OK.
- Click on Apply and then OK to complete the delegation process.

Remember to turn off the delegation of your email account once you return to the office.

If leave is unanticipated and you are unable to setup delegation authority prior to your leave, a request can be submitted to the Information Security's Network Monitoring group to perform this operation on your behalf, including any delegate permissions and adding or maintaining an Out of Office reply. If you are unable to provide direct authorization for any reason, your Director may also submit a request in your absence. For more information regarding this topic, contact Corporate Information Security of the Comptrollership Branch.

# 11. Mailbox Management

## 11.1 Mailbox size and limitations

At the present time, there are no restrictions on the size of your mailbox. However, there is a 15Mb-size limitation on e-mail messages and attachments that you can send. You will be notified automatically when a message exceeds this limit. You should note that there may be circumstances when the e-mail mailbox may not accept a document that is large.

For additional information, contact your local IT support or the National Helpdesk.

## 11.2 File type restrictions



There are restrictions on the file types that can be sent as attachments to your e-mail. All incoming or outgoing e-mail messages containing restricted file types will be delivered without the file attachment. The list of filtered attachments may be adjusted in response to emerging vulnerabilities.

A notice to both the originator and intended recipients will automatically provide notification that the attachment was not delivered. The notice in the header of your e-mail will be something to the effect of:
Outlook blocked access to the following potentially unsafe attachments: FileName.exe

E-mails may also be filtered out by the anti-spam tools. Spam filtering may reject valid e-mail and the user will not receive notification of e-mails blocked by that tool.

### 11.3 Filing your e-mail

You must retain all e-mail messages and attachments that you identify as corporate information. That way, you and your colleagues can access and retrieve them, as necessary.

For additional information, consult the Information Management Directive on the Management of Electronic Mail.

## 12. E-mail Using Wireless Devices

At CBSA, certain devices, such as the BlackBerry, have been approved for wireless e-mail communication. The use of wireless devices is a restricted service approved for managers, directors and executives.

Refer to the CRA link on wireless e-mail for further information.

## 13. Guarding Against Common E-mail Threats

The following are some guidelines for protecting yourself against common e-mail threats.

### 13.1 Viruses, Worms and Trojan Horses

CBSA corporate e-mail is protected by McAfee anti-virus software installed on all Agency desktops and laptops. This also includes a personal firewall which blocks unauthorized outbound network traffic from your desktop (when it becomes infected by a zombie or botnet and is used to launch attacks or forward SPAM). As well, a web filtering application blocks access to common prohibited websites, typically included as links in Spam e-mails and which can be used to infect your computer simply by visiting the website.







These safeguards provide good protection, but should also be supplemented by the following personal measures by users to prevent SPAM or getting infected by through e-mail:

- Don't open attachments (ie. photos, music, docs, links) from unknown e-mails.
- Don't download from file sharing services (ie. limewire, bit torrent, warez, etc.).
- Make sure all outbound e-mails and attachments are scanned for viruses (ie. laptops).

If you believe that your system is infected, you should immediately notify the IT Help Desk as well as report an IT incident (see section 14).

## 13.2 SPAM (Unsolicited e-mail)

When you receive a SPAM (Unsolicited e-mail) message, normally it should immediately be deleted. However, where the message is offensive, unlawful, or cyber crime (such as child pornography and scams), it must be reported to your supervisor and your local IT help desk.

If a spam message is considered a security incident (see section 14), contact CSIAD of the Comptrollership Branch.

SPAM messages to delete:

- Advertisements for pills, software, jewellery, supplies, courses or training, dating services and stock / investments alerts;
- Messages inviting you to visit a certain web site;
- Messages asking for or offering employment.

SPAM messages to report:

- Messages containing images of child pornography or any advertisements or Internet links to that effect;
- Requests for personal information, such as credit card numbers or online banking user ID and password (phishing);
- Messages containing pornographic material;
- Messages involving pyramid schemes.

To reduce SPAM you receive at work, employ the following personal practices:

- Don't forward chain letters to colleagues. Ask them not to forward them to you.
- Don't use your work e-mail to send web cards (i.e. virtual flowers, etc.) to colleagues or friends.
- Don't put your work e-mail on external bulletin boards or social networks such as Facebook (information is known to have been harvested for identity theft and generating SPAM).

## 13.3 Phishing & Social Engineering



Phishing and social engineering are becoming a serious threat to organizations including the CBSA.

**Phishing**
is a form of Internet fraud that uses authentic-looking but false e-mails, websites or other information in order to steal corporate or personal information such as user IDs and passwords, credit card numbers, social insurance numbers, etc.

**Social Engineering**
is the act of manipulating people into performing actions or divulging confidential information.

Phishing and social engineering involve unauthorized individuals attempting to gain access to CBSA electronic resources, data or personal information.

Examples:

A phishing event can involve receiving an e-mail at work, which looks like it might be from the help desk, requesting you to provide your network user id and password through clicking a hyperlink in the e-mail message. If you provide your user id and password, in reality, you are compromising your identification and an unauthorized person will now be able to potentially masquerade as you to access certain network services and gain access to restricted information.

Social engineering is if you receive a phone call at work from someone saying they're from the help desk and they need your user id and password so they can reset your access as part of 'routine maintenance'.

Phishing and social engineering have this in common: they both have an element of sounding official because they're using official letterhead or terms familiar to you.

Tips for preventing phishing and social engineering:

- Never give out your user ID and password to anyone who asks for it by e-mail or over the phone.
- If you feel suspicious, ask for verification of credentials of anyone calling or asking for information, such as their name and telephone. Tell them you'll have to call them back. Then check that they are in fact, employed by CBSA and that they have a need to know this information.
- If you're unsure or in doubt... don't give any information out.
- If you feel you have received a phishing e-mail message or are the victim of phishing or social engineering at work:
  - Tell your supervisor.
  - Report IT Security incidents immediately to your local IT support.

## 13.4 Spoofing



Spoofing occurs when a user receives e-mail that appears to have originated from one source when it actually was sent from another source. Spoofing is often an attempt to trick the user into releasing sensitive information (such as passwords) to what is believed a legitimate site, however the information is sent to a different site.

Examples of spoofing that could negatively affect security include:

- An e-mail message may appear to be from a well-known bank asking recipients to visit a website to confirm their account details, but the website is actually controlled by a hostile party.
- Users' access what seems is a legitimate federal government web page however it has been reproduced in "look and feel". Information provided is sent to another server that is under the control of an attacker.

E-mail spoofing is a form of unsolicited e-mail. Do not open attachments or links contained in an e-mail unless you are certain or can verify the identity of the person or organization that sent you the message. Delete this type of message when in doubt of the originator. You can check the authenticity of the message by opening a new Internet browser session and typing in the correct address of the organization. For related information on spoofing, refer to the Phishing & Social Engineering section above and the Common threats to be aware of Website (to access this site, you need to use a computer with an Internet connection).

## 13.5 Spyware

Spyware is software that is installed on a computer without a user's permission, which intercepts or takes partial control over the user's interaction with the computer. Typically spyware targets the Internet browser (Internet Explorer), causing pop-ups or redirected web pages to appear. Infection can occur through a number of ways, including opening e-mail attachments, clicking links in spam e-mails or visiting certain websites.

Treat Spyware like a virus and follow the measures mentioned in the Viruses, Worms and Trojan Horses section above.

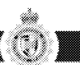
## 13.6 Common E-mail Best Practices

Refer to IT Security for the E-Mail Best Practices Guide on how to appropriately use e-mail and the Frequently asked questions.

# 14. Reporting E-mail IT Security Incidents

When an IT security incident involving e-mail occurs, it must be promptly reported. To find out how to report a security incident, you can access the Corporate Security Intranet site for details on Reporting of Security Incidents.


Canada Border Services Agency
Agence des services frontaliers du Canada



This document was developed for the CBSA by IT Security, Directives and Strategies Division of the Innovation, Science and Technology Branch in collaboration with Corporate Security and Internal Affairs Division of the Comptrollership Branch.

Forward any comments regarding this document to CBSA IT Security.

PROTECTION • SERVICE • INTEGRITY

Canada

Agence des services frontaliers du Canada    Canada Border Services Agency



# Lignes directrices concernant la Directive sur l'utilisation appropriée du courriel

PROTECTION • SERVICE • INTÉGRITÉ

Canada



# 1. Introduction

La Directive sur l'utilisation appropriée du courriel résume les obligations et les responsabilités des utilisateurs pour qu'il utilise le système de courriel de l'ASFC de façon appropriée.

Les services de courriel offerts à l'ASFC et fournis par celle-ci sont réservés aux activités de l'Agence. L'utilisation personnelle à des fins limitées est autorisée à condition de respecter la Politique sur l'utilisation des ressources électroniques de l'ASFC de même que les autres directives et dispositions législatives applicables relevant de l'ASFC ainsi que des gouvernements fédéraux et provinciaux. Les services de courriel font l'objet d'une surveillance et sont assujettis aux exigences et aux demandes liées à l'Accès à l'information et à la protection des renseignements personnels (AIPRP).

Les présentes lignes directrices, qui sont fondées sur la Directive sur l'utilisation appropriée du courriel, sont conçues pour fournir des indications quant à l'utilisation responsable des systèmes et des services de courriel de l'ASFC. Elles soulignent vos principales responsabilités à titre d'utilisateur du système de courriel de l'ASFC et fournissent des exemples concrets sur la façon dont la directive concernant les messages électroniques s'applique à vos activités quotidiennes.

# 2. Courriel de l'ASFC

Le courriel de l'ASFC est réservé à un usage professionnel. Vous devez en être conscient lorsque vous transmettez des messages électroniques. Ceux-ci sont conservés sur les systèmes de l'ASFC même après que l'auteur ou le destinataire les ont supprimés. Également, lorsqu'il est envoyé hors du contrôle des systèmes de l'ASFC, sur l'Internet par exemple, le message électronique peut être intercepté ou modifié, à moins d'avoir été chiffré. Un message électronique envoyé à l'extérieur de l'Agence peut se comparer à une carte postale : n'importe qui peut le lire et l'utilisateur ne doit donc pas s'attendre à ce qu'il reste confidentiel.

Lorsque vous envoyez ou recevez un message électronique :

- Réfléchissez au contenu de votre message, puis rédigez-le et corrigez-le avant de l'envoyer.
- Assurez-vous que chaque personne qui figure sur la liste de distribution a effectivement « besoin de connaître » le contenu du message ou des pièces jointes.
- Si le message contient de l'information de nature délicate, il pourrait être nécessaire de le chiffrer (reportez-vous aux détails ci-après concernant le chiffrement).

Comment, pourquoi, et même quand nous utilisons les services de courriel constituent autant de questions dont nous devons tenir compte dans nos activités de tous les jours. Prenez quelques



instants pour apprendre comment vous pouvez nous aider tous à utiliser au mieux cette importante ressource ministérielle.

## 3. Responsabilités concernant le courriel

Le courriel est devenu un moyen rapide et efficient de communication pour les utilisateurs de l'Agence des services frontaliers du Canada (ASFC). Il est utilisé comme un outil de communication administrative essentiel aux activités et au fonctionnement quotidien de l'Agence. L'information que vous colligez ou que vous créez dans le cadre de vos activités professionnelles appartient à l'ASFC. Voilà pourquoi vous devez tenir compte des activités de l'Agence ainsi que des exigences auxquelles elle doit se plier sur le plan législatif et de la responsabilité lorsque vous traitez le contenu des messages électroniques, tout comme vous le feriez pour de l'information sur papier ou sur tout autre support non électronique.

Lorsque vous utilisez quotidiennement le courriel pour exécuter votre travail, il vous incombe de protéger l'information et les biens de l'ASFC. Les lignes directrices qui suivent résument vos responsabilités. Pour de plus amples détails, reportez-vous à la Directive sur l'utilisation appropriée du courriel.

- N'envoyez aucune information de nature délicate, telle que des renseignements sur les clients ou les employés, au moyen des systèmes de courriel standard de l'ASFC car ils ne sont pas protégés. Il y a des risques potentiels que si de tels renseignements étaient transmis par voie électronique sans mesures de contrôle et de sécurité appropriées, ils pourraient être lus par des personnes non autorisées, ou envoyés par erreur à de telles personnes ou destinations.
- Ne participez à aucune activité criminelle, illégale ou inacceptable. Vous trouverez des exemples de telles activités dans la Politique sur l'utilisation des ressources électroniques ainsi que dans le Code de conduite de l'ASFC.
- Apprenez comment traiter et protéger le courriel, car certains risques sont associés à son utilisation.
- Signalez à votre superviseur tout bris de nature criminelle ou illégale à la sécurité, aux directives ou aux normes informatiques.
- Informez-vous sur toutes les directives, normes et lois applicables relevant de l'ASFC et du gouvernement du Canada.
- Adressez-vous à votre superviseur en cas de doute sur les procédures appropriées et les utilisations acceptables des services et des systèmes de courriel de l'ASFC.

## 4. Utilisation appropriée du système de courriel



Tout valable qu'il soit, le message électronique n'est pas toujours le meilleur outil de communication. Par exemple, vous n'enverrez pas un message concernant le rendement au travail par courriel, mais le livrerez plutôt en mains propres dans le cadre d'une rencontre privée. Lorsque vous devez communiquer de l'information, évaluez s'il serait plus judicieux d'utiliser le téléphone ou de télécopier le message.

Le courriel devenant accessible à une vaste échelle, une « étiquette » du comportement en ligne se dessine.

- Soyez poli. La courtoisie usuelle s'applique à toute communication, qu'elle soit faite par courriel ou en face à face.
- Veillez à être clair et concis.
- L'objet doit être descriptif, mais court.
- Précisez toujours l'action que vous attendez du destinataire.

## 5. Utilisations autorisées du courriel

Les services de courriel doivent servir aux activités officielles visant la réalisation du mandat et de la mission de l'ASFC. Seuls les services et les systèmes de courriel approuvés et appuyés par l'ASFC doivent être utilisés, y compris tout dispositif ayant une fonction de messagerie électronique.

Les services de courriel électronique de l'ASFC doivent être utilisés à des fins appropriées, notamment :

- La communication et le partage de l'information avec des collègues, d'autres ministères ainsi que le secteur privé, dans le cadre de l'exécution des fonctions et des activités de l'ASFC.
- L'utilisation personnelle à des fins limitées. Par exemple, la communication avec des parents, des amis et d'autres personnes à des fins non officielles; l'exécution de transactions bancaires personnelles de routine (pendant les pauses repas, les périodes de repos ou après le travail ou d'autres activités précisées dans le Code de conduite de l'ASFC).

Toute utilisation des services de courriel pour des activités telles que des événements spéciaux ou des envois par listes de distribution doivent être préalablement approuvées par la direction. L'utilisation du courriel pour des avis ou d'autres documents émanant des syndicats doit être préalablement autorisée par les Relations de travail de l'ASFC.

Pour plus de détails sur l'utilisation autorisée du courriel, reportez-vous à la Directive sur l'utilisation appropriée du courriel.



# 6. Utilisations inacceptables ou illégales du courriel

Seuls les services et les systèmes de courriel appuyés et approuvés par l'ASFC doivent être utilisés. Aucun autre fournisseur / système de courriel (par exemple : Hotmail, GMail, Yahoo Mail ou le fournisseur de service personnel de l'utilisateur) ne peut être utilisé.

Vous ne devez pas utiliser le service de courriel de l'ASFC pour créer, stocker, transmettre ou susciter l'envoi de chaînes de lettres, de matériel pornographique ou exercer toute autre activité inappropriée, illicite ou inacceptable du même ordre. Si vous recevez un message électronique non sollicité considéré comme inapproprié en vertu de la définition qui en est faite dans la directive sur le courriel et aux sections 10 et 11 de la Politique sur l'utilisation des ressources électroniques, vous devez le signaler à votre superviseur.

Ne distribuez aucune chaîne de lettres ou pièces jointes contenant des fichiers exécutables ou de gros fichiers (par exemple des images). Si un grand nombre de fichiers ou de documents de ce type sont transmis par le truchement du système de courriel, cela pourrait surcharger les services et précipiter la tombé en panne du système. La reprise du service de courriel pourrait demander beaucoup d'efforts.

Pour consulter d'autres directives et exemples d'utilisation inacceptable du système de courriel de l'ASFC, ainsi que des indications sur les questions liées à la sécurité (comme l'envoi de renseignements protégés), consultez la Politique sur l'utilisation des ressources électroniques et reportez-vous aux directives de l'ASFC en matière de sécurité, que vous trouverez dans le volume Sécurité du Manuel de contrôle.

# 7. Surveillance du courriel

La surveillance à l'ASFC est principalement exercée pour des motifs fonctionnels, à savoir : déterminer si les ressources / réseaux fonctionnent efficacement, repérer et résoudre les problèmes, ainsi que déterminer si l'utilisation est conforme aux directives et aux dispositions législatives relevant de l'ASFC.

Si les activités de surveillance de l'ASFC doivent être menées en conformité avec la *Charte des droits et libertés*, la *Loi sur la protection de la vie privée* et le *Code criminel*, il y a plusieurs raisons pour lesquelles vous ne devriez jamais présumer que votre courriel restera privé. Les communications exécutées par le truchement des ressources de courriel, notamment l'utilisation d'Internet, seront surveillées.

S'il y a lieu de croire qu'une personne utilise à mauvais escient les ressources électroniques de l'Agence, la question est portée à l'attention de la Division de la sécurité de l'Agence et des affaires internes (DSAAI), qui fait enquête. La Division constitue l'autorité fonctionnelle pour ce qui a trait à la surveillance des contenus. La fonction de surveillance des contenus peut inclure la visualisation du contenu et l'analyse du volume des fichiers, des messages électroniques ou des journaux de consignation chaque fois qu'il y a soupçon d'utilisation malveillante.




La DSAAI respecte la confidentialité de l'information et utilise celle-ci uniquement à des fins autorisées comme la conduite d'enquêtes internes à l'ASFC, et en conformité avec les lois applicables.

Pour en savoir davantage, reportez-vous à la Directive sur l'utilisation appropriée du courriel ainsi qu'à la Politique sur l'utilisation des ressources électroniques.

# 8. Types de messages électroniques

À titre d'utilisateur du système de courriel de l'ASFC, vous êtes responsable de la gestion efficace de tous les messages électroniques que vous créez, sollicitez ou transmettez par le truchement de votre boîte aux lettres électroniques. Les messages électroniques sont considérés comme des documents officiels de l'ASFC. Ils doivent être conservés et protégés contre toute destruction ou accès non autorisé.

Les messages électroniques sont considérés comme des renseignements organisationnels ou transitoires. Vous devez prendre les mesures nécessaires pour vous assurer que l'information organisationnelle est saisie comme partie intégrante de la mémoire institutionnelle de l'Agence.

La différence entre les renseignements organisationnels et les renseignements transitoires s'établit comme suit :

## 8.1 Renseignements organisationnels

- Information enregistrée découlant d'actions, de transactions, de processus administratifs, de fonctions et d'activités de l'ASFC.
- Information devant être conservée comme partie intégrante de la mémoire institutionnelle.

## 8.2 Renseignements transitoires

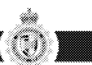
- Information requise pour un temps limité pour s'assurer de l'exécution d'une activité de régie interne ou de la préparation d'un document subséquent.
- Information pouvant être supprimée une fois l'activité de régie interne complétée. Cependant, si une demande d'accès à l'information a été présentée, vous devez conserver l'information jusqu'à ce que le traitement de cette demande soit terminé.

## 8.3 Suppression d'enregistrements de messages électroniques

En règle générale, lorsque l'enregistrement d'un message électronique est supprimé, il n'est pas détruit pour de bon. Ces enregistrements sont habituellement récupérables, même s'ils ont été détruits ou expurgés.







Pout tout complément d'information sur l'information gouvernementale ou temporaire, reportez-vous la Directive sur la gestion des courriels de la Gestion de l'information.

# 9. Classification et étiquetage des messages électronique

## 9.1 Classification des messages électroniques

La classification et l'évaluation de la confidentialité de l'information sont importantes si on veut se prémunir contre la divulgation non autorisée des données de l'ASFC. Les Lignes directrices sur l'utilisation des ressources électroniques comprennent un résumé qui vous aidera à déterminer ce qui est considéré comme protégé (Protégé A, B ou C) et classifié (Confidentiel, Secret et Très secret).

## 9.2 Étiquetage des messages électroniques

Comme pour toutes les autres sortes d'informations, l'objet de l'étiquetage des messages électroniques contenant de l'information de nature délicate consiste à attirer l'attention des utilisateurs pour qu'ils adoptent les mesures de sécurité appropriées.

Si vous êtes l'auteur d'un message électronique, c'est à vous qu'il incombe de lui attribuer le niveau de sécurité approprié (dans l'objet ou sur la première ligne de texte) : non classifié, protégé A ou protégé B.

Également, lorsque la distribution d'un message électronique au-delà de ses destinataires initiaux pose problème, à titre d'expéditeur, vous devez ajouter la mention « Accès restreint » (dans l'objet ou sur la première ligne du texte).

Pour plus de détails, reportez-vous au chapitre 5 du Volume de sécurité, Désignation des renseignements et des biens classifiés et protégés.

# 10. Protection de vos renseignements

## 10.1 Protection de l'information de nature délicate dans les messages électroniques

Avant d'envoyer un message électronique ou une pièce jointe, posez-vous les questions suivantes :

- À quelle catégorie de classification appartient l'information?
- Où le message est-il envoyé?



- Devrait-il être chiffré?

Reportez-vous à la section 9 et aux détails de la section 10 des présentes lignes directrices qui vous aideront à répondre à ces questions. Également, consultez les Lignes directrices sur l'utilisation des ressources électroniques de l'ASFC, ainsi que les chapitres 5, Désignation des renseignements et des biens classifiés et protégés. et 23, Sécurité des communications (COMSEC) du Volume de sécurité.

## 10.2 Quand faut-il chiffrer un message électronique

Les messages électroniques envoyés à l'extérieur du réseau du gouvernement du Canada ne sont pas protégés. Les utilisateurs doivent donc faire attention au contenu des messages qu'ils transmettent hors du système de courriel du gouvernement.

Les communications électroniques doivent être protégées lorsqu'elles sont transmises par le réseau standard de l'ASFC / ARC à un destinataire identifié d'un ministère ou d'un organisme fédéral ou à l'extérieur de l'Agence. Actuellement, l'outil approuvé de chiffrement et de signature numérique est l'ICP (Infrastructure à clé publique) Entrust.

1. Les renseignements non classifiés peuvent être transmis sans autre mesure de contrôle (comme le chiffrement).
2. Les renseignements protégés A peuvent être transmis sans autre mesure de contrôle comme le chiffrement, sauf si leur chiffrement est recommandé en vertu d'une évaluation de la menace et des risques (EMR).
3. Les renseignements protégés B doivent être chiffrés.
4. Les renseignements protégés C ou classifiés ne doivent pas être transmis par un service de courriel standard.

WinZip peut être utilisé pour le chiffrement des pièces jointes aux messages électroniques envoyés à des organismes non gouvernementaux. Le même mot de passe est utilisé par l'expéditeur et le destinataire. Vous devez communiquer ce mot de passe par téléphone régulier (ligne terrestre). Pour de plus amples renseignements, consultez la directive sur le chiffrement des fichiers à l'aide de WinZip (pdf, 2287 Ko).

Si vous avez à traiter des renseignements de niveau protégé C ou supérieur, cherchez conseils et directives auprès de la Division de la sécurité de l'Agence et des affaires internes sur la section de la Sécurité de l'Agence d'Atlas.

Pour en savoir davantage sur l'ICP Entrust, adressez-vous au bureau d'aide de la TI de votre région.

## 10.3 Délégation de vos responsabilités concernant le courriel

Vous ne devez en aucun cas partager votre mot de passe sous prétexte de permettre à quelqu'un d'autre d'accéder à votre compte de courriel. Mais, bonne nouvelle, vous pouvez



partager en toute sécurité votre compte, à des fins professionnelles seulement, en délégant vos droits d'accès sur votre courriel.

MS (Microsoft) Outlook vous permet d'autoriser quelqu'un d'autre à lire, écrire et (ou) modifier des messages sur votre compte, strictement à des fins professionnelles, en votre absence.

Les étapes suivantes expliquent en détail comment activer l'option de délégation et comment choisir les permissions que vous souhaiter déléguer.

- Sur la barre d'outils standard de MS Outlook, cliquez sur Outils, Options.
- Cliquez sur l'onglet Délégués.
- Cliquez sur Ajouter.
- Sélectionnez un nom d'utilisateur dans la liste Nom (carnet d'adresse), puis cliquez sur Ajouter et sur OK.
- Le nom apparaît dans la boîte Ajouter des utilisateurs à droite.
- Une nouvelle boîte apparaît.
- Cliquez sur la flèche vers le bas en regard de l'option Boîte de réception (Inbox) pour déléguer vos permissions.
- Sélectionnez l'une des options (Réviseur, Auteur ou Éditeur).
- Cliquez sur OK.
- Cliquez successivement sur Appliquer et sur OK pour compléter le processus de délégation.

De retour au travail, n'oubliez pas de désactiver la délégation des permissions sur votre compte de courriel.

En cas d'absence imprévue et si vous n'avez pu activer la délégation de vos pouvoirs avant votre départ, une personne peut demander au groupe de la sécurité de l'information responsable de la surveillance du réseau de le faire en votre nom, notamment la délégation de permissions ainsi que l'ajout ou la tenue à jour d'un message de réponse indiquant que vous êtes absent du bureau. Si, pour certaines raisons, vous ne pouvez fournir une autorisation directe, votre directeur peut aussi présenter une demande à cet égard en votre absence. Pour en savoir davantage à ce sujet, communiquez avec la Sécurité de l'information de l'Agence de la Direction générale du contrôle.

# 11. Gestion de la boîte aux lettres

## 11.1 Taille et limites de la boîte aux lettres

À l'heure actuelle, il n'y a aucune restriction quant à la taille de votre boîte aux lettres. Cependant, une limite de 15 Mo est imposée sur les messages électroniques et les pièces jointes que vous pouvez envoyer. Si un message excède cette limite, vous en êtes automatiquement avisé. Sachez aussi que dans certaines circonstances, la boîte aux lettres électronique pourrait refuser un document volumineux.



Pour en savoir davantage, communiquez avec le service de soutien de la TI de votre région, ou le bureau d'aide national.

## 11.2 Restrictions concernant le type de fichier

Certaines restrictions s'appliquent aux types de fichiers que vous pouvez joindre à vos messages électroniques. Tous les messages électroniques entrants ou sortants contenant des types de fichiers faisant l'objet de restriction sont livrés sans leurs pièces jointes. La liste des pièces-jointes filtrées peut être rajustée en réaction à de nouvelles vulnérabilités.

Automatiquement, tant l'auteur que les destinataires prévus reçoivent un avis les informant que la pièce jointe n'a pas été livrée. Cet avis figurant comme en-tête de votre message électronique pourrait ressembler à ceci :
Outlook a blocqué l'accès aux pièces-jointes suivantes susceptibles d'être dangereux :
nomdufichier.exe

Les messages électroniques peuvent aussi être filtrés par les outils anti-pourriel. Lors du filtrage de pourriels, il se peut qu'un message valide soit filtré et l'utilisateur ne recevra pas un avis que son message à été bloqué par cet outil.

## 11.3 Classement de vos messages électroniques

Vous devez conserver tous les messages électroniques et les pièces jointes que vous considérez comme des renseignements organisationnels. Ainsi, vous et vos collègues pourrez y accéder et les récupérer au besoin.

Pour en savoir davantage, reportez-vous à la Directive sur la gestion du courrier électronique de la Gestion de l'information.

# 12. Courriel et appareils sans fil

À l'ASFC, certains appareils tels que le BlackBerry ont été approuvés aux fins de communication sans fil de messages électroniques. Il s'agit là d'un service restreint autorisé aux gestionnaires, directeurs et hauts dirigeants.

Veuillez consulter le lien de l'ARC pour en savoir davantage sur le courriel sans fil.

# 13. Protection contre les menaces les plus courantes en matière de courriel

Voici certaines lignes directrices qui vous permettront de vous prémunir contre les menaces les plus fréquentes que recèlent les messages électroniques.







## 13.1 Virus, vers et chevaux de Troie

Le système de courriel ministériel de l'ASFC est protégé par le logiciel antivirus McAfee, qui est installé sur tous les ordinateurs de bureau et les portables de l'Agence. Ce dispositif inclut également un coupe-feu personnel qui bloque le trafic sur le réseau de matériel non autorisé sortant de votre ordinateur de bureau (lorsque votre ordinateur infecté devenu zombie ou intégré à un réseau de zombies, est utilisé pour lancer des attaques ou faire circuler du pourriel). De même, une application de filtrage Web bloque l'accès aux sites Web communément interdits, qui sont généralement inclus sous forme de liens dans les pourriels et qui peuvent être utilisés pour infecter votre ordinateur (il suffit simplement que vous visitiez le site Web en cause).

Ces mesures assurent une bonne protection, mais doivent également être complétées par les mesures personnelles suivantes, que les utilisateurs doivent prendre pour empêcher la prolifération des pourriels et éviter l'infection par le truchement du courriel :

- N'ouvrez aucune pièce jointe (photos, musique, documents, liens) provenant d'un inconnu.
- Ne téléchargez aucun document provenant d'un service de partage de fichiers (p. ex. : limewire, bit torrent, warez).
- Assurez-vous de passer tous les messages électroniques sortants et leurs pièces jointes à l'antivirus (p. ex. : sur les portables)

Si vous croyez que votre système est infecté, vous devez immédiatement en aviser le bureau d'aide de la TI et signaler un incident de TI (reportez-vous à la section 14).

## 13.2 Pourriel (courriel non sollicité)

Lorsque vous recevez un pourriel (message électronique non sollicité), vous devriez normalement le supprimer immédiatement. Cependant, lorsque le message est offensant, illicite ou qu'il relève de la criminalité cybernétique (pornographie juvénile, escroquerie), vous devez le signaler à votre superviseur et au bureau d'aide de la TI de votre région.

Si un pourriel est considéré comme un incident de sécurité (reportez-vous à la section 14), communiquez avec la DSAAI, Direction générale du contrôle.

Pourriels qui doivent être supprimés :

- Annonces publicitaires pour des pilules, des logiciels, des bijoux, des fournitures, des cours ou de la formation, des services de rencontre et des alertes relatives à des actions / investissements;
- Messages vous invitant à visiter un site Web en particulier;
- Messages demandant ou offrant un emploi.

Pourriels à signaler :

- Messages contenant des images de pornographie juvénile, des annonces ou des liens Internet du même ordre;



- Demande de renseignements personnels, par exemple des numéros de carte de crédit, un nom d'utilisateur et un mot de passe pour des services bancaires en ligne (hameçonnage);
- Messages contenant du matériel pornographique;
- Messages impliquant des opérations pyramidales.

Pour réduire le nombre de pourriels que vous recevez au travail, observez les pratiques personnelles suivantes :

- Abstenez-vous de relayer une chaîne de lettres à vos collègues. Demandez-leur d'en faire autant pour vous.
- N'utilisez pas votre courriel au travail pour envoyer des cartes électroniques (p. ex. : fleurs virtuelles) à vos collègues et amis.
- N'exposez pas votre courriel professionnel sur des babillards externes ou dans des réseaux sociaux comme Facebook (il est avéré que de l'information a été recueillie dans ces lieux à des fins de vol d'identité et de création de pourriels).

## 13.3 Hameçonnage et ingénierie sociale

L'hameçonnage (ou « pêche aux données personnelles ») et l'ingénierie sociale commencent à menacer sérieusement les organisations, notamment l'ASFC.

**L'hameçonnage**

est une forme de fraude sur Internet dans laquelle un faux message électronique, un faux site Web ou une fausse information, qui semble toutefois authentique, est transmis afin de voler des renseignements sur les entreprises et les particuliers, tels que les noms d'utilisateur et les mots de passe, les numéros de cartes de crédit et les numéros d'assurance sociale.

**L'ingénierie sociale**

consiste à manipuler les gens pour qu'ils posent certains gestes ou divulguent des renseignements confidentiels.

Tant dans les cas d'hameçonnage que d'ingénierie sociale, des individus non autorisés tentent d'obtenir accès aux ressources électroniques, aux données ou aux renseignements personnels dont dispose l'ASFC.

Exemples :

Une activité d'hameçonnage peut se traduire par la réception au travail d'un message électronique pouvant sembler provenir du bureau d'aide et dans lequel on vous demande de fournir votre nom d'utilisateur ainsi que votre mot de passe réseau en cliquant sur un hyperlien inséré dans le message. Si vous obtempérez, en fait, vous compromettez vos données d'identification et permettez à une personne non autorisée de se faire passer pour vous pour accéder à certains services sur le réseau et, ce faisant, à de l'information à diffusion restreinte.



On parle d'ingénierie sociale lorsque vous recevez un appel téléphonique au travail d'une personne se faisant passer pour un employé du bureau d'aide et affirmant avoir besoin de votre nom d'utilisateur et de votre mot de passe pour pouvoir réinitialiser vos droits d'accès dans le cadre de l'« entretien de routine ».

Hameçonnage et ingénierie sociale ont en commun leur apparence officielle, du fait qu'ils utilisent du papier à en-tête ou des termes qui vous sont familiers.

Conseils pour se prémunir contre l'hameçonnage et l'ingénierie sociale :

- Ne révélez jamais votre nom d'utilisateur et votre mot de passe à quiconque vous les demande par courriel ou par téléphone.
- En cas de soupçon, demandez à vérifier les justificatifs d'identité, comme le nom et le numéro de téléphone, de toute personne qui vous appelle ou vous demande des renseignements. Dites à cette personne que vous la rappellerez. Vérifiez ensuite si elle travaille effectivement pour l'ASFC ET si elle a besoin de connaître cette information.
- En cas d'incertitude ou de doute... ne révélez aucune information.
- Si vous croyez avoir fait l'objet d'une tentative d'hameçonnage par courriel ou si vous avez été victime d'hameçonnage ou d'ingénierie sociale au travail :
- Dites-le à votre superviseur.
    - Signalez immédiatement tout incident portant atteinte à la sécurité de la TI au service de soutien de la TI de votre région.

## 13.4 Mystification

La mystification se produit lorsqu'un utilisateur reçoit un courriel qui peut sembler provenir d'une source légitime mais qui en réalité en provient d'une autre. D'habitude, le but de la mystification est de tromper les utilisateurs à divulguer des renseignements de nature délicate (comme les mots de passe) à ce qui semble être un site légitime mais qui de fait est envoyé vers un différent site.

Des exemples de mystification qui possiblement nuiraient à la sécurité peuvent comprendre :

- Un message électronique peut sembler provenir d'une banque bien connue et demander aux destinataires de visiter un site web afin de confirmer les détails de leur compte, mais le site web est en fait contrôlé par un parti hostile.
- Des utilisateurs accèdent à ce qui semble être une page web d'un ministère fédéral mais qui en réalité est une reproduction fonctionnelle. Tout renseignement fourni est envoyé à un autre serveur qui est sous le contrôle d'un attaquant.

La mystification de courriel est considérée une forme de courriel non sollicité. N'ouvrez jamais de pièces-jointes et n'accédez pas aux liens contenus dans un courriel sauf dans le cas où vous pouvez assurer l'identité de la personne ou sa provenance. Supprimez tout type de message si vous doutez de l'authenticité de l'expéditeur. Vous pouvez vérifier l'authenticité du message en ouvrant une nouvelle session de navigateur Internet et tapez la bonne adresse web de l'organisation. Pour des renseignements complémentaires concernant la mystification, consultez la section ci-dessus sur l'hameçonnage et l'ingénierie sociale ainsi que le site web Menaces



courantes à connaître (pour accéder à ce site, vous devez utiliser un ordinateur raccordé à Internet).

## 13.5 Logiciels espions

Il s'agit de logiciels installés sur un ordinateur sans l'autorisation de son utilisateur, et qui intercepte ou contrôle partiellement l'interaction entre l'utilisateur et son ordinateur. En règle générale, le logiciel espion cible le navigateur Internet (Internet Explorer), et fait surgir des fenêtres en incrustation ou des pages Web détournées. L'infection emprunte des voies diverses, notamment l'ouverture de pièces jointes à des messages électroniques, ou l'activation de liens insérés dans des pourriels ou la visite de certains sites Web.

Traitez les logiciels espions comme des virus et suivez les mesures susmentionnées dans la section Virus, vers et chevaux de Troie.

## 13.6 Bonnes pratiques reconnues en matière de courriel

Reportez-vous au site web de La sécurité de la TI pour consulter le Guide des bonnes pratiques en matière de courriel concernant l'utilisation appropriée du courriel ainsi que la Foire aux questions (FAQ)

# 14. Incidents de sécurité de la TI concernant le courriel

Lorsqu'un incident de sécurité de la TI concernant un message électronique survient, il doit être signalé sans tarder. Pour savoir comment procéder, accédez au site Intranet de la Division de la sécurité de l'Agence qui explique le signalement des incidents de sécurité.

Le présent document a été rédigé à l'intention de l'ASFC par la Division de la sécurité, des directives et des stratégies des TI, Direction générale de l'innovation, des sciences et de la technologie en collaboration avec la Division de la sécurité de l'Agence et des affaires internes, Direction générale du contrôle.

Veuillez faire part de vos commentaires sur le présent document à la Sécurité de la TI de l'ASFC.

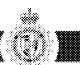
Canada Border Services Agency | Agence des services frontaliers du Canada



# Directive on the Use of Wireless Technology

PROTECTION • SERVICE • INTEGRITY

Canada



# 1. Effective date

This directive is effective immediately upon issuance.

This directive, formerly a policy, replaces version 1.1 (June 5, 2009) and incorporates administrative updates effective May 13, 2013.

# 2. Directive

It is the directive of the Canada Border Services Agency (CBSA) that authorized individuals deploying and / or using Agency wireless devices, systems and services are subject to applicable Government of Canada (GC) and CBSA policies, standards and guidelines. This directive expands and further elaborates upon the security requirements for the use of wireless technology referred to in the CBSA Policy on the Use of Electronic Resources.

# 3. Application

This directive applies to:

a. All wireless technology used by CBSA.
b. All authorized individuals implementing and / or using CBSA wireless technology including devices, systems and services.

# 4. Objective

The aim of this directive is to protect CBSA electronic communications and data assets by ensuring Agency-wide uniformity of measures for the secure design, configuration and use of any device, system or service that utilizes wireless technologies. This directive also provides direction to authorized individuals on the use of CBSA approved wireless devices, systems and services, internal and external to the Agency.

# 5. Context

There has been a high rate of acceptance in the use of wireless technology within CBSA due to its portability, flexibility and convenience. However, as with any technology, wireless devices and communications are potentially vulnerable to threats, vulnerabilities and risks that must be mitigated through the implementation of appropriate safeguards and controls.

The Treasury Board Secretariat (TBS) Policy on Government Security (PGS)* states that departments must have an IT Security strategy designed to protect government assets against rapidly evolving threats that have the potential to impact their confidentiality, integrity, availability, intended use and value. The TBS Policy on the Management of Government



Information* states that departments must protect information throughout its life cycle. The TBS Operational Security Standard: Management of Information Technology (MITS)* states that departments must apply appropriate safeguards and restrict the use of wireless devices to authorized individuals. These requirements and principles will be expanded upon within this Directive.

# 6. Definitions

**Authorized individuals**
include CBSA employees, contractors / consultants and other persons who have been authorized by management to access CBSA's electronic resources, including wireless technology.

**Wireless device**
refers to any portable device used to access electronic resources, systems, services and networks using wireless technology. Wireless devices include, but are not limited to, cellular phones, pagers, laptops, Personal Digital Assistants (PDAs), satellite communication equipment, two way radios, and peripherals (i.e. mice and keyboards).

**Wireless**
refers to any technology that communicates via an air interface such as infrared (IR) or radio frequency transmissions instead of closed wiring paths. For the purposes of this directive, the term wireless includes all devices, systems and services that have wireless connectivity capabilities. This also includes wireless devices as defined above.

# 7. Directive Requirements

The use of wireless technology within CBSA is subject to all applicable Agency and federal laws, legislation, policies and standards. The use of wireless technologies for classified information is also subject to the *Security of Information Act**. Under the *Access to Information Act** and the *Privacy Act**, individuals may have access to electronic records, subject to applicable exemptions under those acts.

To ensure a secure working environment within CBSA, security measures must be implemented when using wireless technology. The measures consist of the following key security components:

a. Security planning and architecture
b. Lifecycle management
c. Use by Authorized individuals

## 7.1 Security Planning & Architecture



a. The planning and deployment of any wireless technology within CBSA must include the active participation and advice / guidance of the Agency IT Security Coordinator.
b. All wireless technology is subject to IT Security Risk Management, (refer to the CBSA IT Security Risk Management Policy), prior to production to ensure unacceptable risks are identified and mitigated.
c. The architecture of any wireless technology must include technical security controls as required by applicable IT Security policies, standards and guidelines.

## 7.2 Lifecycle Management

a. Security requirements of any wireless technology deployed within the Agency must be identified and included in any technical design document and / or relevant project and system documentation.
b. Wireless technology deployed by the Agency must permit the monitoring, logging and storage of any electronic records created, stored or transmitted via wireless devices, systems and services.
c. All information created, received or transmitted via wireless technology including devices, systems or services in the normal course of CBSA operations and that contains information on Agency functions, actions and decisions must be preserved in accordance with the TBS Policy on the Management of Government Information.
d. Electronic communications and records generated by wireless technology are subject to the *Access to Information Act* and *Privacy Act*, and may be accessed by individuals making an ATIP request, subject to applicable exemptions under these Acts.
e. Any wireless technology deployed in CBSA is subject to IT Security Certification & Accreditation prior to deployment.

## 7.3 Use by Authorized Individuals

a. Only Agency-approved wireless technology devices, systems and services may be used to conduct government business, to communicate with other government employees and with the public, to gather information relevant to their duties, to develop expertise in using such resources and limited personal use as described in the Policy on the Use of Electronic Resources. Wireless technology devices, systems and services may only be used by authorized individuals for CBSA business purposes.
b. Individuals must turn off wireless devices with a voice transmission capability when attending a meeting at which sensitive information, above Protected A, is being shared.
c. Authorized individuals who use CBSA wireless systems and services must observe the prohibitions against criminal, unlawful and unacceptable activities outlined in the Policy on the Use of



Electronic Resources and this directive and must comply with all applicable legislation, policies and guidelines.

d. Individuals violating this directive are subject to disciplinary action up to and including termination of employment, as outlined in the Policy on the Use of Electronic Resources.

# 8. Roles and responsibilities

The roles and responsibilities described below are in addition to those identified in the Policy on the Use of Electronic Resources.

## 8.1 Authorized Users

Authorized users of wireless technology are responsible for:

a. Using wireless technology devices, systems and services in accordance with GC and Agency policies, standards and guidelines; and
b. Taking reasonable measures to safeguard wireless technology and associated data in their care and responsibility against theft, compromise or unauthorized access.

## 8.2 Managers

Managers are responsible for:

a. Authorizing the use of approved wireless technology for operational requirements; retrieving wireless devices from users and discontinuing wireless services when no longer required, authorized or upon leaving the Agency; and
b. Reporting all suspected violations of this directive to the Departmental Security Officer (DSO).

## 8.3 Director General, Infrastructure Services Directorate

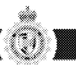
The Director General (DG) of Infrastructure Services Directorate is responsible for:

a. Establishing rules and guidelines governing the use and / or acquisition of wireless technology in accordance with GC and CBSA IT Security policies, standards, guidelines, and / or upon the advice and guidance of the IT Security Coordinator.
b. Ensuring that all wireless technology utilised within CBSA is subject to IT Security risk management, IT Security testing and certification and accreditation prior to deployment.

## 8.4 IT Security Coordinator (ITSC)







The IT Security Coordinator is responsible for:

a. Developing IT Security policies, standards and guidelines to protect wireless technology used by the Agency; and
b. Providing IT Security advice and guidance to managers and senior management for securing wireless technology used by the Agency.

## 8.5 Departmental Security Officer (DSO)

The Departmental Security Officer is responsible for:

a. Investigating reports of suspected criminal, unlawful or unacceptable uses of CBSA's wireless technology including devices, systems and services.

## 8.6 Contracting, Assets and Telecommunications

Telecommunications is responsible for:

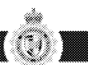
a. Formulating policy for the acquisition and use of wireless telecommunication devices.

# 9. Directive Review

This directive document shall be reviewed at least every five years under the authority of the IT Security Coordinator and the Departmental Security Officer (DSO).

# 10. References

CBSA Policy on the Use of Electronic Resources
CBSA Directive on the Appropriate Use of E-mail
CBSA Guidelines for the Directive on the Use of Wireless Technology
Cellular Telephone Policy
CSEC - Government of Canada Wireless Vulnerability Assessment (ITSB-02))
CSEC - Bluetooth Vulnerability Assessment (ITSPSR-17)
CSEC - Personal Digital Assistant Vulnerability Assessment (ITSPSR-18)
*Security of Information Act*
CSEC - Security of BlackBerry Pin-to-Pin Messaging (ISTB-57)
CBSA Addendum - Use of PIN-to-PIN on BlackBerry devices
Appendix - Additional Security Requirements for Wireless Devices



For additional applicable references, consult Section 17 of the CBSA Policy on the Use of Electronic Resources.

# 11. Enquiries

Enquiries regarding this directive should be directed to:

IT Security and Continuity
Information, Science & Technology Branch
E-mail: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca
Intranet: IT Security
Security and Professional Standards Directorate
Comptrollership Branch
E-mail: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

All questions regarding CBSA cellular phones, satellite communication equipment, and other IT system-independent telecommunication devices should be forwarded to the Contracts, Assets and Telecommunications Division of the Comptrollership Branch.

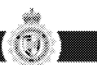
Agence des services frontaliers du Canada | Canada Border Services Agency



# Directive sur l'utilisation de la technologie sans fil

PROTECTION • SERVICE • INTÉGRITÉ





# 1. Date d'entrée en vigueur

La présente directive entre en vigueur dès sa diffusion.

Cette directive, anciennement une politique, remplace la version 1.1 (05 juin 2009) et intÃ¨gre des mises Ã  jour administratives Ã  compter du 13 mai 2013.

# 2. Directive

L'Agence des services frontaliers du Canada (ASFC) a pour politique que les personnes autorisées qui mettent en place ou utilisent des appareils, des systèmes et des services sans fil de l'Agence sont visées par les politiques, les normes et les lignes directrices pertinentes du gouvernement du Canada (GC) et de l'ASFC. La présente directive développe et explique les exigences en matière de sécurité touchant l'utilisation de la technologie sans fil dont fait mention la Politique sur l'utilisation des ressources électroniques de l'ASFC.

# 3. Application

La présente directive porte sur :

a. Toute la technologie sans fil utilisée par l'ASF.
b. Toutes les personnes autorisées qui mettent en place ou utilisent des technologies sans fil de l'ASFC, dont des appareils, des systèmes et des services

# 4. Objet de la directive

L'objectif de la présente directive est de protéger les communications électroniques et des données de l'ASFC en assurant l'uniformité des mesures à la grandeur de l'Agence visant la conception, la configuration et l'utilisation des appareils, systèmes et services qui utilisent la technologie sans fil. La directive contient aussi des directives à l'intention des personnes autorisées qui utilisent les appareils, systèmes et services sans fil, internes et externes, approuvés par l'Agence.

# 5. Contexte

L'utilisation de la technologie sans fil est très répandue à l'ASFC en raison de sa portabilité, de la flexibilité et de sa commodité. Toutefois, les appareils et les communications sans fil sont vulnérables à des menaces, dangers et risques qui doivent être atténués par la mise en place de protections et de contrôles appropriés.

La Politique sur la sécurité du gouvernement* (PSG) du Secrétariat du Conseil du Trésor (SCT) précise que les ministères doivent avoir une stratégie de sécurité de la TI pour sauvegarder les actifs gouvernementaux contre des menaces qui changent rapidement et ont le potentiel








d'affecter la confidentialité, l'intégrité, la disponibilité, l'usage prévu et la valeur de ces systèmes. La Politique sur la gestion de l'information gouvernementale* du CST précise que les ministères doivent protéger l'information durant son cycle de vie. La norme sur la sécurité opérationnelle du CST, La gestion de la sécurité des technologies de l'information (GSTI)* mentionne que les ministères doivent mettre en place des protections appropriées et restreindre l'utilisation des appareils sans fil aux personnes autorisées. La présente directive développe ces exigences et principes.

# 6. Définitions

**Personnes autorisées**

comprennent les employés de l'ASFC, les entrepreneurs et d'autres personnes qui ont été autorisées par la direction à utiliser les ressources électroniques de l'ASFC dont les technologies sans fil.

**Appareil sans fil**

s'entend de tout appareil portable utilisé pour accéder aux ressources, systèmes, services et réseaux électroniques au moyen de technologies sans fil. Les appareils sans fil comprennent, entre autres, les téléphones cellulaires, les téléavertisseurs, les portables, les assistants numériques personnels, le matériel de communication satellitaire, les émetteurs-récepteurs et les périphériques, notamment les souris et claviers.

**Sans fil**

désigne toute technologie qui communique par interface aérienne, dont les fréquences infrarouges ou radio, au lieu de suivre des trajets fermés composés de fils et de câbles. Aux fins de la présente directive, l'expression sans fil s'entend aussi des appareils, systèmes et services qui ont une capacité de connexion sans fil ainsi que des appareils sans fil définis plus haut.

---

* Pour accéder à ce site, vous devez utiliser un ordinateur raccordé à Internet.

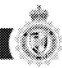
# 7. Exigences de la directive

L'utilisation de la technologie sans fil à l'ASFC est assujettie à toutes les lois, à tous les textes législatifs, à toutes les politiques et à toutes les normes applicables de l'Agence et du gouvernement fédéral. L'utilisation de la technologie sans fil pour la transmission de renseignements classifiés est également soumise à la *Loi sur la sécurité de l'information**. En vertu de la *Loi sur l'accès à l'information** et de la *Loi sur la protection des renseignements personnels**, une personne peut avoir accès aux dossiers électroniques, sous réserve des exemptions applicables prévues par ces lois.

Pour offrir un milieu de travail protégé à l'ASFC, des mesures de sécurité doivent être mises en œuvre pour l'utilisation de la technologie sans fil. Ces mesures comprennent les composantes de sécurité clés suivantes :







a. planification et architecture de sécurité
b. gestion du cycle de vie
c. utilisation par des personnes autorisées

## 7.1 Planification et architecture de sécurité

a. La planification et le déploiement de toute technologie sans fil à l'ASFC doivent comprendre la participation active du coordonnateur de la sécurité de la TI et la prise en compte de ses conseils et avis.
b. Toute technologie sans fil est soumise à la gestion des risques à la sécurité (consulter la Gestion des risques pour la sécurité - Évaluation de la menace et des risques des technologies de l'information), avant sa production afin que les risques inacceptables soient cernés et atténués.
c. L'architecture de toute technologie sans fil doit comprendre les contrôles de sécurité technique exigés par les politiques, normes et lignes directrices de sécurité de la TI.

## 7.2 Gestion du cycle de vie

a. Les exigences en matière de sécurité de toute technologie sans fil implantée à l'Agence doivent être établies et comprises dans tout document de conception technique ou toute documentation de projet ou de système pertinent.
b. La technologie sans fil mise au point par l'Agence doit permettre la surveillance, l'enregistrement et le stockage des dossiers électroniques créés, stockés ou transmis par appareils, systèmes et services sans fil.
c. L'information créée, reçue ou transmise par technologie sans fil, dont des appareils, systèmes et services dans le cours normal des opérations de l'ASFC et qui contient des renseignements sur les fonctions, actions ou décisions de celle-ci doit être sauvegardée conformément à la Politique sur la gestion de l'information gouvernementale du CST.
d. Les communications et dossiers électroniques produits par la technologie sans fil sont visés par la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*, et une personne peut y avoir accès, sous réserve des exemptions applicables prévues par ces lois.
e. Toute technologie sans fil mise au point par l'Agence est soumise à la certification et à l'accréditation de sécurité de la TI avant son déploiement.

## 7.3 Utilisation par des personnes autorisées

a. Seuls les appareils, systèmes et services sans fil approuvés par l'Agence peuvent être utilisés pour mener des affaires du gouvernement, communiquer avec d'autres employés du







gouvernement et des membres du public, recueillir de l'information pertinente à leurs fonctions, acquérir une expertise dans l'utilisation de ces ressources et pour des fins personnelles limitées telles que précisées dans la Politique sur l'utilisation de ressources électroniques. Les appareils, systèmes et services sans fil ne peuvent qu'être utilisés par les personnes autorisées pour la conduite des affaires de l'AFSC.

b. Les utilisateurs doivent éteindre leurs appareils sans fil capables de transmettre des messages vocaux lorsqu'ils assistent à une réunion où de l'information délicate (protégée et ayant une cote supérieure à A est échangée.
c. Les personnes autorisées qui utilisent des systèmes et des services sans fil de l'ASFC doivent observer les mesures de protection contre les activités criminelles, illégales et inacceptables qui sont exposées dans la présente directive et la Politique sur l'utilisation des ressources électroniques et respecter tous les textes législatifs, politiques et lignes directrices applicables.
d. Les personnes qui enfreignent la présente directive pourront faire l'objet de mesures disciplinaires allant jusqu'à la cessation d'emploi, tel qu'il est exposé dans la Politique sur l'utilisation des ressources électroniques.

---

* Pour accéder à ce site, vous devez utiliser un ordinateur raccordé à Internet.

# 8. Rôles et responsabilités

Les rôles et responsabilités décrits ci-dessous s'ajoutent à ceux définis dans la Politique sur l'utilisation des ressources électroniques.

## 8.1 Utilisateurs autorisés

Les utilisateurs autorisés utilisant la technologie sans fil sont responsables de ce qui suit :

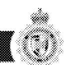
a. Utiliser la technologie sans fil, dont les appareils, les systèmes et les services, selon les politiques, les normes et les lignes directrices du GC et de l'Agence;
b. Prendre des mesures raisonnables pour protéger la technologie sans fil et leurs données contre le vol, l'atteinte à son intégrité ou l'accès non autorisé.

## 8.2 Gestionnaires

Les gestionnaires sont responsables de ce qui suit :







a. Autoriser l'acquisition et l'utilisation de la technologie sans fil pour des besoins opérationnels valides et récupérer les appareils mobiles des utilisateurs ou interrompre les services lorsque ces appareils ne sont pas requis ou autorisés ou lorsque les utilisateurs quittent l'Agence.
b. Signaler les violations présumées de la présente directive à l'agent de sécurité du ministère (ASM).

## 8.3 Directeur général, Direction des services d'infrastructure

Le Directeur général (DG) de la Direction des services d'infrastructure est responsable de ce qui suit :

a. Établir les règles et les lignes directrices régissant l'utilisation et / ou l'acquisition de la technologie sans fil conformément aux politiques, normes et lignes directrices de sécurité du GC et de l'ASFC et / ou selon les conseils et avis du coordonnateur de la sécurité de la TI.
b. Veiller à ce que toute la technologie sans fil utilisée au sein de l'ASFC fasse l'objet d'une gestion du risque de la sécurité de la TI, d'une mise à l'essai de la TI, d'une certification et d'une accréditation avant son déploiement.

## 8.4 Coordonnateur de la sécurité de la TI (CSTI)

Le coordonnateur de la sécurité de la TI est responsable de ce qui suit :

a. Élaborer des politiques, normes et lignes directrices pour protéger la technologie sans fil utilisée par l'Agence.
b. Fournir des avis et des conseils aux gestionnaires et à la haute direction concernant la protection de la technologie sans fil utilisée par l'Agence.

## 8.5 Agent de sécurité du ministère (ASM)

L'agent de sécurité du ministère est responsable de ce qui suit :

a. Enquêter sur les cas signalés d'utilisation criminelle, illégale ou inacceptable présumée de la technologie sans fil de l'ASFC, ce qui comprend les appareils, systèmes et services.

## 8.6 Contrats, biens et télécommunications

Les Télécommunications sont responsables de ce qui suit :

a. Élaborer la politique sur l'acquisition et l'utilisation des appareils de télécommunication sans fil.







## 9. Examen de la directive

Le présent document de directive sera examiné au moins une fois à tous les cinq ans sous la gouverne du Coordonateur de Sécurité de la TI, et de l'agent de sécurité du ministère.

## 10. Références

Politique sur l'utilisation des ressources électroniques
Directive sur l'utilisation appropriée du courriel
Lignes directrices relatives à la Directive sur l'utilisation de la technologie sans fil
Politique de téléphones cellulaires
CSTC - Gouvernement Évaluation de la vulnérabilité des systèmes de communication sans fil du gouvernement du Canada (ITSB-02)
CSTC - Évaluation de la vulnérabilité de Bluetooth (ITSPSR-17)
CSTC - Évaluation des vulnérabilités des assistants numériques personnels (ITSPSR-18)
*Loi sur la protection de l'information*
CSTC- Sécurité de la messagerie BlackBerry NIP à NIP (ISTB-57)
CBSA Addenda – Utilisation de la messagerie NIP à NIP sur les appareils BlackBerry
Annexe - Exigences supplémentaires en matière de sécurité pour les appareils sans fil

L' article 17 de la Politique sur l'utilisation des ressources électroniques de l'ASFCl'ASFC fournit d'autres références.

## 11. Demandes de renseignements

Les demandes de renseignements au sujet de la présente directive doivent être adressées au :

Sécurité et continuité de la TI
Direction générale de l'information, des sciences et de la technologie
Courriel: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca
Intranet: Sécurité de la TI

Direction générale du contrôle
Direction de la sécurité et des normes professionnelles
Courriel: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Les questions portant sur les téléphones cellulaires, le matériel de communication et les autres appareils de télécommunications étrangers au réseau de la TI doivent être adressées à la Division des contrats, des biens et des télécommunications de la Direction générale du contrôle.






Canada Border Services Agency
Agence des services frontaliers du Canada



# Guidelines for the Directive on the Use of Wireless Technology

PROTECTION • SERVICE • INTEGRITY

Canada



# 1. Introduction

The aim of the Directive on the Use of Wireless Technology is two-fold:

- To protect Canada Border Services Agency (CBSA) wireless electronic communications and transmitted data by ensuring Agency-wide uniformity for the secure design, configuration, deployment and use of any CBSA device, system or service that utilizes wireless technologies.
- To provide direction on the use of CBSA approved wireless devices, systems and services. Wireless technology, like any CBSA electronic resource, is to be used appropriately by all Agency users.

These guidelines, based on the Directive on the Use of Wireless Technology, are intended to provide guidance about the secure deployment and responsible use of CBSA wireless technology. It outlines key responsibilities for users of CBSA wireless devices, systems and services. All users who utilize wireless technology at CBSA should familiarize themselves with this Directive.

# 2. Wireless Technology at CBSA

There has been a high rate of acceptance in the use of wireless technology within CBSA due to its portability, flexibility and convenience. CBSA supported and approved devices and services that utilize wireless technologies are to be used for official business purposes.

These guidelines will help you understand what wireless technology is, the common security threats associated with wireless devices and how to securely use approved CBSA wireless electronic resources at CBSA. Please take a few moments to learn what you can do to help all of us make best use of this important corporate resource.

# 3. Overview of Wireless Technology

Wireless technology, in its simplest form, enables one or more devices to communicate without physical connections - without requiring network or peripheral cabling. Wireless technologies use radio, infrared or microwave frequency transmissions as the means for transmitting data, whereas traditional wired technologies use cables. Wireless networks allow devices to be moved about with varying degrees of freedom and still maintain communication with each other. They also offer greater flexibility than cabled networks and significantly reduce the time and resources needed to set up new networks and allow for ad hoc networks to be easily created, modified or torn down.

However, there are risks which are inherent with using wireless technology. Perhaps the most significant source of risk in wireless networks is that the technology's underlying communication medium, the airwave, is open to electronic eavesdropping, making it the equivalent of installing a wired network connection outside your building that anyone can access. Wireless signals can travel through the walls, ceilings and windows of buildings up to hundreds of metres outside of the building walls. If these signals are not protected, they are accessible by anyone within a

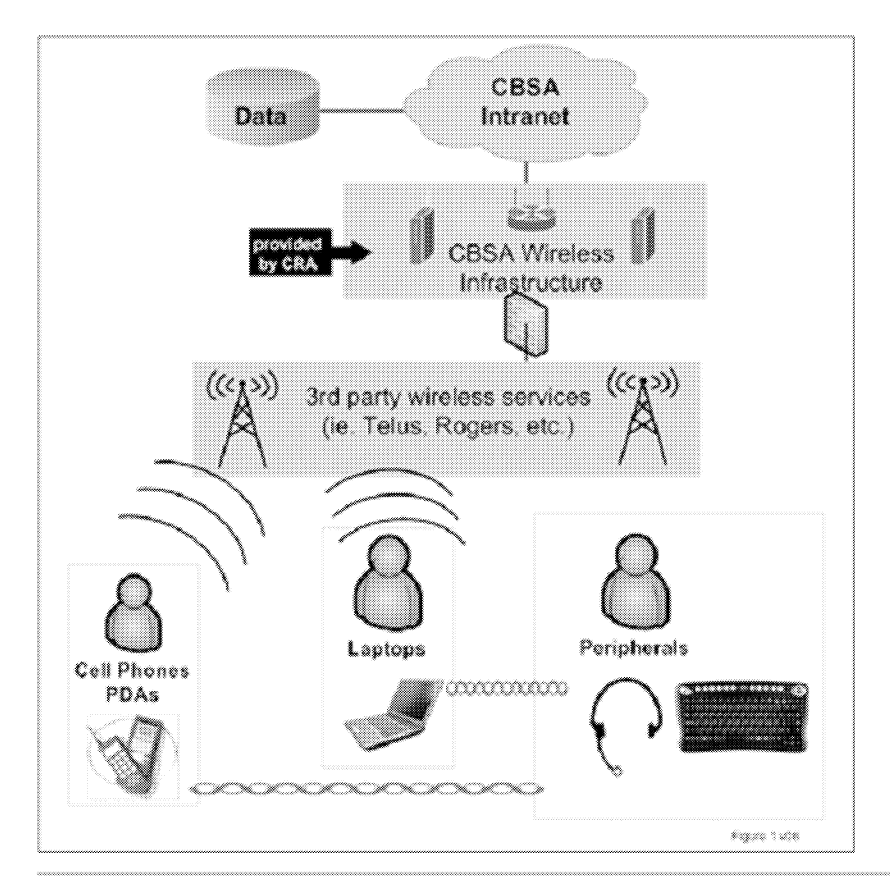


range thereby providing an access point to the CBSA network beyond the physical security controls of the wired network.

# 4. Components Associated with Wireless Technologies

Figure 1 provides a simplified representation of the many potential components associated with wireless technologies deployed by CBSA. It focuses on user requirements for securing wireless devices, such as laptops, cellular phones and other devices. It does not provide guidance for hardening a wireless network or installation of the components. Currently CBSA has a Service Level Agreement with the Canada Revenue Agency (CRA) to provide the secure wireless network infrastructure necessary for authorized wireless devices to connect to the Agency network.[1]

## Figure 1 - Representative Wireless Technology Components




[1]CRA has developed Security Standards and Guidelines for wireless networks, and complies with applicable Government of Canada (GC) Policies and Standards. CRA Wireless Networks Standard - 2005



# 5. Categories of Wireless Devices

Wireless technologies range from complex systems such as Wireless Local Area Networks (WLAN) and mobile phones including the new generation of 3G mobile phones, to simple devices such as wireless headphones, microphones, remote sensors and other devices that do not process or store information.

They also include Infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link and allow communication. Wireless networks serve as the transport mechanism between devices and other devices and traditional wired networks (enterprise networks and the Internet).

For simplicity, wireless devices can be broken into four categories.

1. Cellular Phones, many manufacturers
2. Personal Digital Assistants (PDAs) e.g. Blackberry - Rogers and TELUS
3. Laptops, many makes and models
4. Peripherals e.g. Keyboard and mouse, Headsets

# 6. User Responsibilities

The use of wireless technology provides flexibility and an efficient means of communication for CBSA users. As a user, you have a responsibility to protect sensitive information and assets. Wireless connectivity creates new security risks that you need to understand in the ordinary fulfillment of your daily business job requirements.

You are the best protection available by being aware of your personal IT security responsibilities, conforming to policies, and by the diligent use of security techniques. We are all expected to use common sense and good judgment in our work and interaction with colleagues, clients and the public.

The directives and guidelines on the Use of the Electronic Resources and the Appropriate Use of E-mail outline many of your responsibilities. In addition to those, here is a summary of your responsibilities as they relate to wireless technology. Please refer to the Directive on the Use of Wireless Technology for further details.

a. Do not send sensitive information such as client and employee information using wireless devices and systems because they are not secure[2]. There are potential risks that sensitive information could be read by, intercepted or misdirected to unauthorized persons and destinations if such information is transmitted electronically without the proper controls and safeguards. Refer to



section 7 of these guidelines that details the risks and threats associated with wireless devices.

b. Learn how to manage and protect the information that you process or transmit on wireless devices.
c. Personal use of CBSA-owned cellular telephones is authorized only under exceptional circumstances or in emergency situations. Refer to the CBSA Cellular Telephone Policy for further details.
d. You must not connect any personally owned wireless devices to the CBSA network.
e. Do not use wireless devices to access office voice mailboxes or retrieve voice messages as the password to your office voicemail could be detected.
f. Wireless devices that have digital camera, microphone or recording capabilities are not to be used in any area that processes protected and/or classified information.
g. Wireless devices and communications shall be turned off in situations where sensitive information is being discussed or electronically processed. Computer systems and their peripherals (i.e. printer, projector) emanate radio waves, which can be intercepted and analyzed to recover sensitive information. Devices with wireless communications operated in close proximity to such equipment become excellent vehicles for broadcasting sensitive information, which could then be intercepted and exploited.
h. Do not engage in activities that are criminal, unlawful, or unacceptable. You can find some examples of these activities in the Policy on the Use of Electronic Resources and in the CBSA Code of Conduct.
i. Report any criminal or unlawful breach of computer security, policies, and standards to your supervisor.
j. Be informed of all CBSA and Government of Canada applicable policies, standards and laws.

2For further information regarding the secure transmission of sensitive information via wireless technology, refer to Chapter 23 of the Security Volume, Communication Security (COMSEC) Policy.

# 7. Security Concerns with Wireless Devices

Wireless devices and technology provide many productivity benefits. but they also pose new risks to the CBSA as an organization, which must be managed. This section provides an overview of the common IT security concerns with wireless technology.

While the Agency has invested heavily in deploying technical safeguards to protect networks, infrastructure and data, with wireless technology these controls can potentially be bypassed by users. Therefore, it is very important that everyone in the organization is aware of the potential information leakage which can result from the use of wireless technology, and ensure that



appropriate user preventative measures (see Sections 6, 9 and Appendix A) are taken to prevent such occurrences.

Once the threats are understood to wireless technology and devices, users can supplement the existing network and infrastructure technical controls through protective measures they can take individually in order to provide the greatest possible protection of Agency systems, information and networks.

Mobile wireless devices such as cellular phones, PDAs and laptops, are potentially vulnerable to a range of security threats including:

- electronic eavesdropping;
- electronic tracking;
- loss, theft, or disposal;
- unauthorized access;
- signal jamming;
- malware; and,
- SPAM

Cellular phones and PDAs also face additional threats due to:

- Size and portability
- Available wireless interfaces and associated services

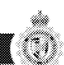
The size and portability of a wireless device can result in the loss of physical control of a device. Once in the physical possession of an unauthorized user, with enough time and effort, many types of security mechanisms can be overcome or bypassed to gain access to the data contained on a device. Wireless interfaces such as cellular and Bluetooth also provide alternative means for exploitation. Stolen wireless devices with active services can result in accumulated financial charges or used to commit fraud. They can also be used to deliver malicious software (malware) to other wireless devices.

## Summary of Threats to Various Wireless Devices

| Threat | Description | Examples |
|---|---|---|
| **Electronic eavesdropping** | Electronic Interception of cellular phone conversations. Install spyware onto a device to collect and forward information onto another phone or server. | • Certain cellular phone models offer spyware applications to monitor voice communications.<br>• Hackers can perform war driving where a hacker drives around in a car with a portable wireless device looking for unprotected entry points into wireless networks.<br>• Hackers can configure a |







| | | |
|---|---|---|
| | | laptop to impersonate a legitimate wireless access point in an airport lounge or coffee shop allowing client connections to be attracted and sensitive data collected. |
| **Electronic tracking** | Geographic location tracking of holders of wireless devices. | • Location tracking services are offered by several companies for cellular phones.<br>• GPS device location on Blackberry. |
| **Loss, theft or disposal** | Because of their small size, wireless devices, can be lost or stolen. Care must be taken for disposing (i.e. reusing/recycling) of wireless devices and that all data is erased. | • A stolen wireless device with active service could be used to place toll and international calls and accumulate charges for the subscriber.<br>• A stolen wireless device can be resold for profit on eBay, with the memory contents available for recovery.<br>• Tools are available to recover erased data from the flash memory (define or simply by removing "flash") of most current cellular phones. |
| **Unauthorized Access** | Access to a device and its contents can be gained by forging or guessing a PIN or password. | • Tools exist to bypass built-in security and recover contents of a device. |
| **Signal jamming** | RF (radio frequency) communications are susceptible to flooding attacks causing a denial-of-service attack. This normally involves overloading network resources and denying normal operation of the target | • A flooding attack could force a PDA to resynchronize, allowing unwanted and unauthorized users to join the network. |



| | | |
|---|---|---|
| | network. | |
| **Malware** | Typically mobile malware targets smart phones and PDAs. | • Internet downloads - downloading an infected file disguised as a game, security patch, utility or other useful application from a freeware site.<br>• Messaging services - malware can be attached to e-mail and then launched if attachment is opened.<br>• Bluetooth - malware can be delivered when a Bluetooth-enabled device is placed in discoverable mode. |
| **Spam** | Unwanted SMS (Short messaging service) text messages, e-mail and voice messages on mobile phones. | • SPAM can be used for phishing attempts to entice users into revealing passwords, financial details or other private info via web pages, text messages or to download malware attached to a message or via a web page. |

## Cameras

Cameras (motion or still), are becoming common in wireless devices such as cellular phones and PDAs. However, built-in cameras pose unique threats.

Using a personal wireless camera device, motion or still photos can be taken of network topology drawings (i.e. white board sketches or plotter drawings) and sent to an external device (i.e. another phone or PDA) undetected and without raising suspicion. This information can then be used for the planning and execution of a successful external hacking attack on the network.

Potential targets of interest by a perpetrator with a personal wireless camera device could also include server room locations, physical access controls, power/HVAC (heating, ventilation and air conditioning) sources and even physical security controls such as cameras and guard posts. Photos of these kinds could be used to bypass security controls and execute a physical break-in resulting in the theft of servers, equipment and information.



In classified areas, an internal perpetrator could take screen captures using a digital cellular phone camera of classified information, which could be used by external threat agents, such as organized crime, to gain knowledge allowing them to thwart CBSA procedures and investigations or bypass customs and excise collection.

While these examples only just touch on the possible targets of opportunity, which can be impacted by unauthorized use of cameras on wireless devices, they do demonstrate the clear threat from wireless technology, particularly as these kinds of wireless devices continue to come bundled with ever-expanding features in the future.

### Headsets

Wireless headsets are becoming more popular for use while driving. They come in a wide range of designs and use radio waves and infrared technology. Emanations from headphones, such as verbal telephone discussions and digital recordings, (i.e. audio recordings) are transmitted through the air to the headset from the wireless device (i.e. cellular phone, PDA, laptop, etc.)

Corporate espionage (i.e. stealing secrets from an organization) is an increasingly common practice by many organizations and foreign governments. Using a variant on war-driving, adversaries are known to conduct electronic eavesdropping against senior executives and officers, listening into unencrypted conversations and information by following nearby as they drive. Capable adversaries such as Foreign Intelligence Services and organized crime are also able to intercept and decipher even encrypted cellular phone conversations.

## 8. Use of Wireless Technologies and Devices within CBSA

Wireless devices are valuable tools. They are assigned according to business and operational needs. You are permitted to use wireless devices, systems and services, as defined in CBSA policies and these guidelines, to fulfil work responsibilities and further the CBSA mandate.

Please remember the following general points:

- Transmission of Protected B information must be encrypted and protected with CBSA approved encryption and digital signature mechanisms.
- Protected C or Classified information must never be created, stored or transmitted via wireless technology without completing the Certification and Accreditation process in consultation with the Security and Professional Standards Directorate (SPSD) and ITSCD. Protected C or Classified information requires more stringent safeguards that are to be authorized and approved by the SPSD.
- Personally owned wireless devices, a device not provided or authorized by the CBSA, should not be used for conducting CBSA business nor used on the CBSA premises.

At the present time, a number of wireless services and devices are supported and approved for use at the CBSA.  Where non authorized wireless technologies, services and devices are necessary to fulfill business requirements, IT Security and Continuity Division, in collaboration with ISTB stakeholders, and Security and Professional Standards Directorate may authorize them



on a case by case basis, based on the recommendations of an IT Security risk assessment, and implementation of additional safeguards, where necessary.

## Bluetooth

Bluetooth earpieces/headsets are permitted for CBSA BlackBerry handheld devices. Refer to the CRA Wireless Email (BlackBerry) site for details on how to enable Bluetooth on the BlackBerry device.

For additional information, consult the Instructions on how to set up BB Bluetooth.

## Peripherals

### Wireless Headsets connected to cellular phones (while travelling in vehicles)

Legislation has been passed in certain provinces that prohibit the use of cellular phones while travelling in a vehicle. A hard-wired earpiece can be used in vehicles to provide connectivity. In addition, a Bluetooth earpiece/headset or carkits for BlackBerry can be used. Refer to the CRA Wireless Email (BlackBerry) for details regarding the Agency approved use of wireless for BB.

### Cellular Telephones, Satellite Communication Equipment or Cordless Phones

Cellular phones, as well as satellite communication equipment and cordless phones, may be used for the storage, retrieval and transmission of non-sensitive information via voice messaging. However, when the retrieval of office voice mailbox messages requires the use of a password, access code or PIN, such retrieval is not allowed. These authentication controls are considered sensitive and can be easily intercepted and compromised.

Cellular phones, including satellite communication equipment and cordless phones, must not be used for the storage, retrieval or transmission of voice or data at the Protected A, B or C or classified levels, notably retrieval of office voice mailbox messages. Additionally, cellular phones must not be used for Web browsing and other forms of Internet access (i.e. connecting to an Internet Service Provider [ISP]. Cellular phones must not be used for image capture (motion or still) or as a sound recording device. Text messaging is not permitted unless explicitly approved by CBSA.

### Pagers

Pagers may be used for the storage, retrieval and transmission of non-sensitive information only.

### Agency Approved BlackBerry (BB) Handheld Devices



The BlackBerry is a wireless device which includes an e-mail solution for the CBSA authorized users. BB devices provided by the CBSA allow users to store, retrieve and transmit e-mail messages up to Protected "B" sensitivity when the communications are within the CBSA internal systems. PKI services are enabled and allow users to encrypt e-mails to send secure e-mail messages. In addition to the e-mail functionality, the following services are permitted:Â  SMS (text messaging), PIN-to-PIN voice communications and digital camera capabilities. SMS, PIN-to-PIN and voice communications on the BB devices are not secure; therefore text messaging phone conversations must be limited to non-sensitive information.

Digital camera image capture (still or motion) must not be used to capture sensitive images such as network configurations, facilities or the CBSA personnel. Images which are considered inappropriate, offensive, illegal Â or those which otherwise could reflect negatively upon the Agency should also not be taken.

Refer to the CRA Wireless Email site for further details. For the CBSA, refer to the section "CBSA approval process". Consult the following for a comprehensive list of user guidance documents and approved services for BlackBerry.

CBSA Addendum - Use of PIN-to PIN on BlackBerry Devices

PIN is defined as Personal Identification Number

## Mobile Laptops

CBSA wireless Secure Remote Access (SRA) services on the CBSA provided laptops are approved.Â  Refer to the CRA Secure Remote Access site for further details.

## Wireless Pointing Devices

The use of wireless pointing devices such as laser pointers is authorized.

## Wireless Keyboards

Wireless keyboards are not authorized.

## Other Devices with Image or Voice Recording Capabilities

All other wireless devices not included in these Wireless Technology Guidelines, as well as the corresponding policy, that have digital camera capabilities, microphones or recording capabilities are not authorized to be used within the Agency.

Note: All questions regarding the CBSA cellular phones, satellite communication equipment and other IT system-independent telecommunication devices should be forwarded to the Contracts, Assets and Telecommunications Division of the Comptrollership Branch.



# 9. User Security Measures for Common Wireless Device Threats

This section includes additional security measures that you can apply to protect against common wireless device threats.

1. Understand the sensitivity of information in your wireless communications. Don't discuss or store Protected C or classified information on common cellular phones, PDAs and laptops. Consult with the Security and Professional Standards Directorate for guidance on classified information.
2. Don't change your security settings. Security settings that come with Laptops and PDAs are correctly configured for security when you first receive them.
3. Don't download software to cellular phones, PDAs and laptops. Downloaded software could include malicious code. This includes ringtones, file-sharing (i.e. Kazaa), and other customizable features.
4. Don't post your cellular phone number and email address. Attackers often browse web sites for email addresses and cellular phone numbers. By limiting the number of people who have access to your information, you limit spam and your risk of becoming a victim.
5. Don't follow links sent in email or text messages. Be suspicious of URLs sent in unsolicited email or text messages. What may appear to be legitimate links may actually direct you to a malicious web site.
6. Physical security in the Office. Lock up all laptops, PDAs and wireless devices when you're not in your office. Keep them out of view.
7. Physical security when travelling. Don't leave cellular phones, laptops and PDAs unattended in public areas. Don't check them as baggage. Carry them in inconspicuous baggage not resembling a laptop case.
8. Encrypt your data. If your wireless device is stolen, thieves won't be able to read your data. CBSA approved laptops come with hard disk encryption. If keeping data separate from wireless devices by storing on a thumb-drive, use only approved USB storage devices that can be encrypted.
9. Use strong passwords. Choose passwords that are difficult to guess. At least 8 characters, including a number, an upper and a lower case letter and a symbol (#, !, &)
10. Immediately Report Lost or Stolen Wireless Devices.
    - Report the loss or theft of a wireless device to your local IT support in order to have the device deactivated from the wireless network.



- You should also notify your supervisor and if this is a security incident you must also report it to the Security and Professional Standards Directorate.

## 10. Reporting IT Security Incidents

When an IT security incident involving e-mail occurs, it must be promptly reported. To find out how to report a security incident, you can access the Security and Professional Standards Directorate on Atlas for details on: "How to Report Security Incidents".

An IT security incident is any activity involving, for example:

- Suspected or actual compromise of protected and / or classified information.
- Malicious codes and virus alerts / attacks against CBSA communication or computer systems or other circumstances leading to system degradation (do not forward files or email if you think you have a virus, call the IT help desk).
- Theft, loss, compromise or destruction of information, wireless devices, systems or services, or other related assets belonging to, or in the care of CBSA.
- Incidents involving wireless technology, suspected of constituting unacceptable, illegal or criminal offences.
- Incidents involving wireless technology that have an impact on government operations or that could, as a result, require revisions to operational standards or technical documentation.

## 11. Summary

Wireless technologies are rapidly changing and the Agency will continue to evaluate secure wireless solutions for CBSA on an ongoing basis. These guidelines will be updated periodically to reflect changes in the technology and the associated security measures for protecting wireless technology solutions adapted by the Agency.

## 12. Enquiries

This document was developed for the CBSA by IT Security and Continuity Division of the Information, Science and Technology Branch in collaboration with the Security and Professional Standards Directorate of the Comptrollership Branch.

Forward any comments regarding this document to CBSA IT Security:
E-mail: CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca and Intranet

## 13. Abbreviations

| | |
|---|---|
| 1G | First Generation (mobile phones) |







| | |
|---|---|
| 3G | Third Generation |
| CSEC | Canadian Security Establishment Canada |
| IEEE | Institute of Electrical and Eletronics Engineers |
| IR | Infrared |
| IrDA | Infrared Data Association |
| MB | Mobile Broadband |
| MBWA | Mobile Broadband Wireless Access |
| RF | Radio Frequency |
| WiFi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WMAN | Wireless Metropolitan Area Network |
| WMAX | Wireless Interoperability for Microwave Access |
| WPAN | Wireless Personal Area Networks |
| WWAN | Wireless Wide Area Networks |

# 14. Definitions

| Term | Definition |
|---|---|
| 1G | 1G is the first generation of mobile phones and is analog. |
| 3G | 3G is the third generation of mobile phone standards and technology, superseding 2G, and preceding 4G. It is based on the International Telecommunication Union (ITU) family of |





| | |
|---|---|
| | standards. 3G networks are wide area cellular telephone networks which evolved to incorporate high-speed internet access and video telephony. |
| Bluetooth | A wireless short-range radio communications technology facilitating data transmission over short distances from fixed and mobile devices, creating wireless personal area networks (PANs). |
| IEEE 802.11 | A set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands. IEEE 802.11 networks are short range, high-bandwidth networks primarily developed for data. |
| Infrared | Infrared (IR) radiation is electromagnetic radiation whose wavelength is longer than that of visible light, but shorter than that of terahertz radiation and microwaves. |
| IrDA | In Information and Communications Technology , IrDA refers to Infrared Data Association, a standard for communication between devices (such as computers, PDAs and mobile phones) over short distances using infrared signals |
| Phishing | Phishing refers to impersonation of a trusted person or organization in order to steal a person's personal information, generally for the purpose of identity theft. For example, an e-mail message may appear to be from a well-known bank asking recipients to visit a website to confirm their account details, but the website is actually controlled by a hostile party. |
| WiFi | The trade name for the popular wireless technology [802.11) used in home networks, mobile phones, video games and more. |
| WiMAX | WiMAX, the Worldwide Interoperability for Microwave Access, is a telecommunications technology that provides for the wireless transmission of data in a variety of ways, ranging from point-to-point links to full mobile cellular-type access. It is a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL |
| Wireless LAN | A wireless LAN or WLAN is a wireless local area network, which is the linking of two or more computers or devices without using wires. |



| | |
|---|---|
| Wireless Metropolitan Area Network | WMAN, Wireless Metropolitan area networks are a type of wireless network that connects several Wireless LANs. WiMAX is the term used to refer to wireless MANs and is covered in IEEE 802.16d/802.16e. |
| Wireless Personal Area Networks | WPAN, represents wireless personal area network with a very short range. The reach of a WPAN is typically a few meters. WPANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the internet (an uplink). |
| Mobile Broadband | Mobile broadband is the name used to describe various types of wireless high-speed internet access through a portable modem, telephone or other device. Various network standards may be used, such as WiMAX, UMTS/HSPA, EV-DO and some portable satellite-based systems. |
| Mobile Broadband Wireless Access | See Mobile Broadband above. On 11 December 2002, the IEEE Standards Board approved the establishment of IEEE 802.20, the Mobile Broadband Wireless Access (MBWA) Working Group. The mission of IEEE 802.20 is to develop the specification for an efficient packet based air interface that is optimized for the transport of IP based services. The goal is to enable worldwide deployment of affordable, ubiquitous, always-on and interoperable multi-vendor mobile broadband wireless access networks that meet the needs of business and residential end user markets. |
| Wireless Wide Area Networks | WWAN, which stands for Wireless Wide Area Network, is a form of wireless network. A WWAN differs from a WLAN (wireless LAN) in that it uses cellular network technologies such as WIMAX |

# 15. References and Further Reading

* To access these sites, you need to use a computer with an Internet connection.

CRA Wireless Networks Standard (2005).
CSEC: ITSB-49 Keyloggers and Spyware (May 2008) *
CSEC: ITSPSR17a Bluetooth Vulnerability Assessment (June 2008) *
NIST SP800-124 Guidelines on Cellular Phone and PDA Security (July 2008) * English only.



NIST SP800-121 Guide to Bluetooth Technology (July 2008) * English only.
NSA: Bluetooth Security (Dec 2007) * English only.
NSA: So your boss bought you a new laptop... How do you Identify and disable wireless capabilities? (May 2007) * English only.
Public Safety Canada: General Best Practices for Laptop Security (13 Feb 2008) *
CRA: Wireless Email Solution Acceptable Use Policy (Nov 28, 2007)
CRA: Blackberry Operations Guide (23 July 2007)
CBSA: Cellular Phone Policy (01 April 2008)
Blackberry: Security Technical Overview Blackberry Devices with Bluetooth Technology (18 June 2008) *
USCERT: Cybersecurity for Electronic Devices (20 Aug 2008) * English only.
USCERT: Defending Cellular Phones and PDAs against attack (9 Aug 2006) * English only.
USCERT: Protecting Portable Devices Data Security (10 Oct 2007) * English only.
CRA: User Reference Guide Telus Mobile Wireless Services (v1.0) *
CSEC - Security of BlackBerry Pin-to-Pin Messaging *



# Appendix A - Ways for Business Users to Protect Mobile Wireless Devices

## In Your Office

1. Keep all wireless devices locked in your office or secured to a desk or other appropriate point. If left unattended, use an appropriate locking mechanism (i.e. Ensure your laptop computer is locked in the docking station or PDA is in a filing drawer.)
2. Don't assume that locking your office door is enough protection. As with any item of value, you need to properly secure them in your office while you're away from it.

## While Traveling

1. Never leave mobile wireless devices unattended where you run the risk of forgetting it or having someone pick up the item. At airport security checkpoints don't place on conveyor until you are ready to pass through the metal detector unobstructed.
2. Don't loan your mobile wireless device to someone unfamiliar to you.
3. Don't add file-sharing software (i.e. Kazaa, Limewire, etc.) or any other unauthorized software on mobile wireless devices.
4. Don't keep passwords and account numbers on mobile wireless devices or share them with anyone.
5. Carry laptops or other wireless mobile devices in a generic carrying bag or luggage to disguise the contents.
6. Never check your laptop or other mobile wireless mobile device as baggage on any commercial carrier (plane, train, etc.) or at the bell station or luggage holding area of a hotel.
7. Never put laptops or other mobile wireless devices in the trunk of a taxi or in the luggage rack of a limo / shuttle.
8. Lock your laptop or other mobile wireless device in the trunk of rental cars while traveling, but secure it in your room or keep it with you if you'll be away from the car for an extended period or overnight.
9. Use hotel or room safes to secure a mobile wireless device or if you must leave unattended.
10. Always remember that wireless traffic can be intercepted by anyone out of thin air. There is no wire that needs to be tapped.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Lignes directrices relatives à la Directive sur l'utilisation de la technologie sans fil

PROTECTION • SERVICE • INTÉGRITÉ





# 1. Introduction

L'objectif de la Directive sur l'utilisation de la technologie sans fil est double :

- Elle vise à protéger les communications et la transmission de données électroniques sans fil de l'Agence des services frontaliers du Canada (ASFC) en garantissant une uniformité de procédure dans l'ensemble de l'Agence pour ce qui est de la conception, de la configuration, du déploiement et de l'utilisation sécuritaires de tout appareil, système ou service de l'ASFC qui s'appuie sur les technologies sans fil.
- Elle fournit une orientation quant à l'utilisation des appareils, systèmes et services approuvés par l'ASFC. La technologie sans fil, comme toute autre ressource électronique de l'ASFC, doit être utilisée adéquatement par tous les utilisateurs de l'Agence.

Les présentes lignes directrices, basées sur la Directive sur l'utilisation de la technologie sans fil, visent à fournir des directives concernant le déploiement sécuritaire et l'utilisation responsable des technologies sans fil de l'ASFC. Elles décrivent les principales responsabilités des utilisateurs des appareils, systèmes et services de l'ASFC. Tous ceux qui ont recours à la technologie sans fil à l'ASFC devraient se familiariser avec cette directive.

# 2. La technologie sans fil à l'ASFC

Le taux d'acceptation relatif à l'utilisation de la technologie sans fil a été très élevé à l'ASFC en raison de la portabilité, de la souplesse et de la commodité qui la caractérisent. Les appareils et services soutenus et approuvés par l'ASFC qui font appel aux technologies sans fil doivent être utilisés à des fins professionnelles officielles.

Les présentes lignes directrices vous aideront à comprendre en quoi consiste la technologie sans fil, quelles sont les menaces à la sécurité courantes associées aux appareils sans fil, et comment utiliser en toute sécurité à l'Agence les ressources électroniques sans fil approuvées par l'ASFC. Prenez quelques instants pour apprendre comment vous pouvez nous aider tous à utiliser au mieux cette importante ressource organisationnelle.

# 3. Aperçu de la technologie sans fil

La technologie sans fil, dans sa forme la plus simple, permet à un ou plusieurs dispositifs de communiquer entre eux sans connexion – sans qu'il soit nécessaire de recourir à un câblage de réseaux ou de périphériques. Les technologies sans fil utilisent les transmissions par radiofréquences, fréquences infrarouges ou micro-ondes pour transmettre des données, alors que les technologies câblées classiques utilisent des câbles. Les réseaux sans fil permettent de déplacer des dispositifs selon divers degrés de liberté tout en maintenant la communication entre ces derniers. Ils offrent également une plus grande souplesse que les réseaux câblés et réduisent sensiblement le temps et les ressources nécessaires pour constituer de nouveaux réseaux, en plus de permettre de créer, modifier ou détruire facilement des réseaux spéciaux.

Cependant, il existe des risques inhérents à l'utilisation de la technologie sans fil. Peut-être la plus importante source de risque dans les réseaux sans fil provient-elle de la technologie sous-jacente de ce moyen de communication, à savoir les ondes, qui sont ouvertes à l'interception





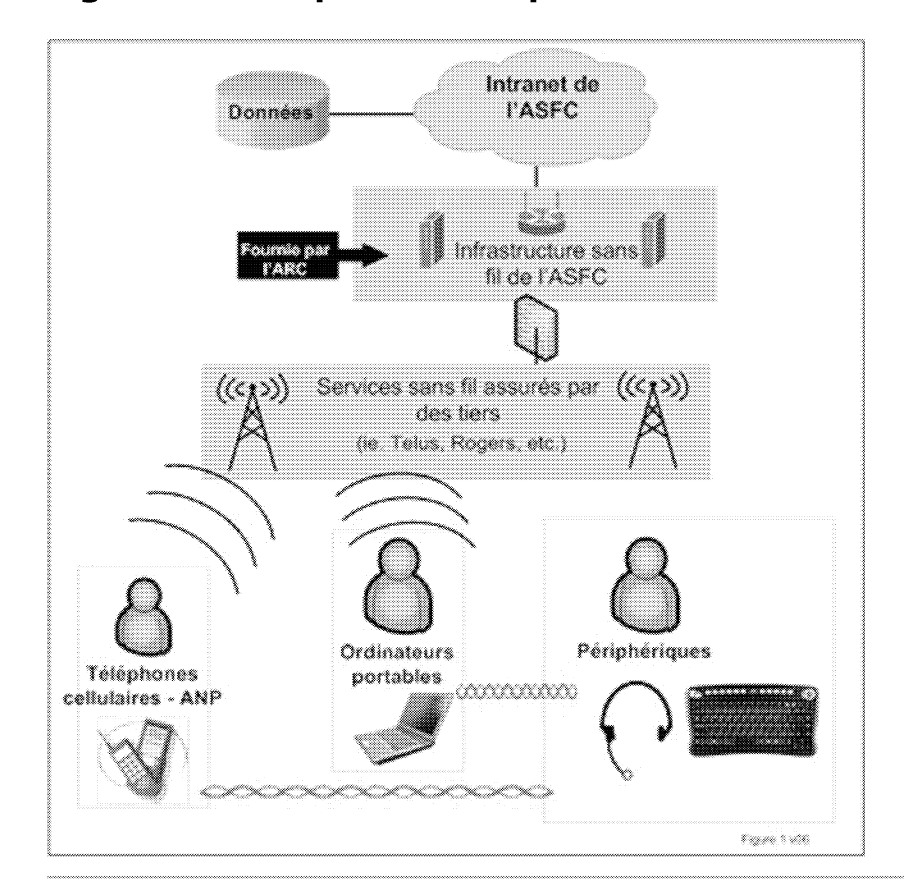


illicite, ce qui revient à installer à l'extérieur d'un immeuble un réseau câblé auquel n'importe qui peut accéder. Les signaux sans fil peuvent traverser les murs, les plafonds et les fenêtres des édifices jusqu'à des centaines de mètres des murs. Si ces signaux ne sont pas protégés, ils sont accessibles à quiconque à l'intérieur d'un certain rayon et fournissent un point d'accès au réseau de l'ASFC qui échappe aux contrôles de sécurité physiques du réseau câblé.

# 4. Éléments des technologies sans fil

L'illustration de la Figure 1 fournit une représentation simplifiée des nombreuses composantes qui peuvent être associées aux technologies sans fil déployées par l'ASFC. Elle met l'accent sur la nécessité, pour les utilisateurs, de sécuriser les appareils sans fil comme les ordinateurs portables et téléphones cellulaires. Elle n'établit pas de directives pour le renforcement de la sécurité d'un réseau sans fil, ni pour l'installation des composantes. L'ASFC a conclu un accord sur les niveaux de service avec l'Agence du revenu du Canada (ARC) afin de fournir l'infrastructure de réseau sans fil nécessaire pour que les dispositifs sans fil autorisés puissent se connecter au réseau de l'Agence.[1]

## Figure 1 - Composantes représentatives des technologies sans fil










1L'ARC a mis au point des normes et lignes directrices relatives à la sécurité des réseaux sans fil, et respecte les politiques et normes applicables du gouvernement du Canada. ARC – Norme relative à la sécurité du réseau sans fil - 2005

# 5. Catégories d'appareils sans fil

Les technologies sans fil vont des systèmes complexes comme les réseaux locaux sans fil (WLAN) et les téléphones sans fil, dont la nouvelle téléphonie cellulaire de troisième génération, aux simples dispositifs comme les écouteurs sans fil, les microphones, les télécapteurs et autres appareils qui ne traitent pas et n'emmagasinent pas d'information.

Ce type de technologie comprend également les dispositifs infrarouges (IR) comme les télécommandes, certains claviers et certaines souris sans fil, et les casques stéréo haute fidélité sans fil, qui nécessitent tous un trajet de visibilité directe entre un émetteur et un récepteur pour établir le lien et permettre la communication. Les réseaux sans fil servent de mécanismes de transport entre des appareils et d'autres appareils et réseaux câblés classiques (réseaux des entreprises et Internet).

Pour simplifier les choses, les appareils sans fil peuvent être divisés en quatre catégories.

1. Téléphones cellulaires (nombreux fabricants)
2. Assistants numériques personnels (ANP) par exemple, Blackberry - Rogers et TELUS
3. Ordinateurs portables, grand nombre de marques et de modèles d'ordinateurs portables
4. Périphériques par exemple, Clavier et souris, Casques d'écoute

# 6. Responsabilités des utilisateurs

L'usage de la technologie sans fil permet une certaine souplesse et fournit un moyen de communication efficace aux utilisateurs de l'ASFC. En tant qu'utilisateur, vous avez la responsabilité de protéger les renseignements et les biens de nature délicate. La connectivité sans fil crée de nouveaux risques de sécurité que vous devez comprendre dans le cours de l'accomplissement normal de vos tâches quotidiennes.

Vous constituez la meilleure protection possible en étant conscient de vos propres responsabilités en matière de sécurité des TI, en vous conformant aux directives et en appliquant minutieusement les techniques de sécurité. Nous sommes tous censés faire preuve de sens logique et de jugement dans nos interactions avec nos collègues, les clients et le public.

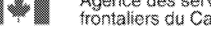
Les directives et lignes directrices concernant l'utilisation des ressources électroniques et l'utilisation appropriée du courriel décrivent bon nombre de vos responsabilités. De plus, voici un résumé de vos responsabilités par rapport à la technologie sans fil. Consultez la Directive sur l'utilisation de la technologie sans fil pour plus de précisions.





a. N'envoyez aucune information de nature délicate, comme des renseignements sur les clients ou les employés, au moyen des appareils ou systèmes sans fil, car ils ne sont pas protégés[2]. Il y a des risques potentiels que, s'ils étaient transmis par voie électronique sans mesures de contrôle et de sécurité appropriées, de tels renseignements pourraient être lus par des personnes non autorisées, ou envoyés par erreur à de telles personnes ou destinations. Reportez-vous à la section 7 de ces lignes directrices, où l'on expose en détail les risques et menaces associés aux appareils sans fil.
b. Apprenez comment gérer et protéger l'information que vous traitez ou transmettez au moyen d'appareils sans fil.
c. L'usage à des fins personnelles de téléphones cellulaires appartenant à l'ASFC est autorisé seulement en cas de circonstances exceptionnelles ou de situations d'urgence. Reportez-vous à la Politique de téléphones cellulaires de l'ASFC pour plus de détails.
d. Vous ne devez connecter aucun appareil sans fil personnel au réseau de l'ASFC.
e. N'utilisez pas d'appareil sans fil pour accéder à votre boîte vocale au bureau ou pour écouter vos messages vocaux, car le mot de passe de votre répondeur pourrait ainsi être détecté.
f. Les appareils sans fil comportant un appareil photo numérique, un microphone ou un dispositif d'enregistrement ne doivent pas être utilisés dans un endroit où l'on traite de l'information protégée ou classifiée.
g. Vous devez éteindre les appareils sans fil et mettre fin à une communication sans fil dans des situations où l'on discute ou traite électroniquement des informations sensibles. Les systèmes informatiques et leurs périphériques (p. ex. : imprimante, projecteur) émettent des ondes radio qui peuvent être interceptées et analysées afin de récupérer de l'information sensible. Les appareils recourant à la communication sans fil qui sont utilisés très près de ces équipements deviennent d'excellents véhicules de diffusion d'information sensible, laquelle pourrait alors être interceptée et exploitée.
h. Ne participez à aucune activité criminelle, illégale ou inacceptable. Vous trouverez des exemples de telles activités dans la Politique sur l'utilisation des ressources électroniques ainsi que dans le Code de conduite de l'ASFC.
i. Signalez à votre superviseur tout bris de nature criminelle ou illégale à la sécurité, aux politiques ou aux normes informatiques.
j. Informez-vous sur toutes les politiques, normes et lois applicables relevant de l'ASFC et du gouvernement du Canada.

[2] Pour de plus amples renseignements concernant la transmission sans fil sécurisée de renseignements de nature délicate, consultez le Chapitre 23 du Volume de sécurité, Politique sur la Sécurité des communications (COMSEC).






# 7. Préoccupations de sécurité concernant les appareils sans fil

Les appareils et la technologie sans fil offrent de nombreux avantages sur le plan de la productivité, mais ils posent aussi de nouveaux risques pour l'ASFC en tant qu'organisme, des risques qui doivent être gérés. Cette section fournit une vue d'ensemble des préoccupations courantes en matière de sécurité des TI relativement à la technologie sans fil.

Bien que l'Agence ait fortement investi dans le déploiement de mesures de protection techniques afin de protéger les réseaux, l'infrastructure et les données, avec la technologie sans fil, ces contrôles pourraient être contournés par les utilisateurs. Par conséquent, il est très important que tout le monde dans l'organisme soit au courant de la possibilité de fuites d'information que pourrait entraîner l'utilisation de la technologie sans fil, et de veiller à ce que les utilisateurs prennent les mesures préventives (voir les sections 6, 9 et l'annexe A) qui s'imposent pour prévenir de tels cas.

Une fois qu'ils auront compris en quoi consistent les menaces posées aux technologies et appareils sans fil, les utilisateurs pourront compléter les contrôles techniques des réseaux et de l'infrastructure par des mesures de protection qu'ils pourront appliquer de manière individuelle pour assurer la plus grande protection possible des systèmes, de l'information et des réseaux de l'Agence.

Les appareils sans fil mobiles comme les téléphones cellulaires, les ANP (PDA) et les ordinateurs portables sont potentiellement vulnérables à toute une série de menaces à la sécurité, dont :

- l'écoute électronique;
- la surveillance électronique;
- la perte, le vol ou l'élimination;
- l'accès non-autorisé;
- le brouillage de signal;
- les maliciels; et
- les pourriels.

Les téléphones cellulaires et ANP sont également visés par des menaces additionnelles pour les raisons suivantes :

- Leur taille et de leur portabilité
- Les interfaces sans fil et services connexes disponibles

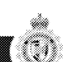
La taille et la portabilité d'un appareil sans fil peuvent entraîner la perte de contrôle physique d'un dispositif. Une fois l'appareil en possession d'un utilisateur non autorisé, si l'on y met suffisamment de temps et d'efforts, on peut déjouer ou venir à bout de nombreux types de mécanismes de sécurité pour accéder aux données contenues dans un appareil. Les interfaces sans fil telles que les technologies cellulaires et Bluetooth fournissent d'autres moyens d'exploiter l'information. Les appareils sans fil volés dont les services sont actifs peuvent entraîner une accumulation de frais ou servir à commettre une fraude. Ils peuvent également être utilisés pour transmettre des logiciels malveillants (maliciels) à d'autres appareils sans fil. Le Tableau 2 ci-dessous résume les menaces courantes relatives aux appareils sans fil.





# Sommaire des menaces aux différents appareils sans fil

| Menace | Description | Exemples |
|---|---|---|
| **Écoute électronique** | Interception électronique de conversations par téléphone cellulaire. Installe un logiciel espion dans un appareil pour recueillir l'information et la transmettre à un autre téléphone ou serveur. | • Certains téléphones cellulaires offrent des applications de logiciel espion permettant de contrôler les communications vocales.<br>• Les pirates informatiques peuvent faire du « war driving », c'est-à-dire circuler en voiture avec un appareil portable sans fil à la recherche de points non protégés pour accéder à des réseaux sans fil.<br>• Les pirates peuvent, pour recueillir des données confidentielles, configurer un ordinateur portable en points d'accès légitimes à un réseau sans fil dans un café d'aéroport afin d'inciter les usagers de tels réseaux à s'en servir. |
| **Surveillance électronique** | Géolocalisation des détenteurs d'appareils sans fil. | • Plusieurs compagnies offrent des services de géolocalisation des téléphones cellulaires.<br>• Dispositif de localisation GPS sur Blackberry. |
| **Perte, vol ou élimination** | En raison de leurs petites dimensions, les appareils sans fil peuvent être facilement égarés ou volés. Faire preuve de prudence lors de l'élimination (réutilisation ou recyclage) ou l'effacement de toutes les données. | • Un appareil sans fil volé et qui est toujours en service peut servir à faire des appels à l'étranger, ce qui augmentera les frais facturés à l'abonné.<br>• Un appareil sans fil volé peut être revendu sur eBay pour des raisons pécuniaires et le contenu de la mémoire peut être récupéré.<br>• Il existe des moyens de récupérer les données |



| | | |
|---|---|---|
| | | effacées de la mémoire flash (en définissant ou en enlevant tout simplement « flash ») de la plupart des téléphones cellulaires actuels. |
| **Accès non autorisé** | Il est possible d'accéder à un appareil et à son contenu en créant ou en retrouvant un NIP ou un mot de passe. | • Il existe des moyens de contourner les dispositifs de protection incorporés et de récupérer le contenu d'un appareil. |
| **Brouillage de signal** | Les communications (radiofréquence) sont susceptibles d'inondations causant une attaque entraînant un déni de service. Ce type d'attaque consiste normalement à surcharger les ressources d'un réseau l'empêchant de fournir ses services habituels. | • Une inondation peut forcer la resynchronisation du PDA permettant à des utilisateurs indésirables et non autorisés d'accéder au réseau. |
| **Logiciel malveillant** | Le logiciel malveillant mobile cible habituellement les téléphones intelligents et les PDA. | • Téléchargements dans Internet – téléchargement d'un fichier contaminé présenté faussement sous forme de jeu, de correctif de sécurité, d'utilitaire ou de toute autre application utile téléchargés d'un site offrant des logiciels gratuits.<br>• Services de messagerie – un logiciel malveillant peut être joint à un courriel et installé à l'ouverture du fichier joint.<br>• Bluetooth – un logiciel malveillant peut s'installer quand un appareil utilisant Bluetooth est en mode découverte. |
| **Pourriel** | Réception non voulue de SMS (service d'envoi de messages | • Le pourriel peut servir à des tentatives |



| | | |
|---|---|---|
| | courts), de messagerie texte, de courriels et de messagerie vocale sur des téléphones cellulaires. | d'hameçonnage pour inciter les utilisateurs à révéler leurs mots de passe, des détails financiers ou d'autres informations confidentielles par le biais de pages Web, de messages textes ou à télécharger un logiciel malveillant joint à un message ou téléchargé à partir d'une page Web. |

## Caméras

Les appareils sans fil tels que les téléphones cellulaires et les PDA sont de plus en plus dotés de caméras et d'appareils photographiques. Ce type de caméra et d'appareils photographiques incorporés posent toutefois des problèmes de menace uniques.

Il est possible, avec un appareil sans fil, de photographier ou filmer des dessins de la topologie de réseau (c.-à-d., esquisses sur tableau blanc ou dessins de traceur) et les transmettre à un dispositif externe (un autre téléphone ou un PDA) sans être détecté et sans éveiller de soupçons. Ces renseignements peuvent ensuite être utilisés par un pirate informatique pour planifier et exécuter avec succès une attaque contre le réseau.

Les emplacements de la salle des serveurs, les contrôles de l'accès physique, les sources d'alimentation CVCA (chauffage, ventilation et conditionnement d'air) et même les points de contrôle tels que les caméras et les postes de surveillance pourraient être des cibles potentielles d'un malfaiteur muni d'un appareil portatif doté d'un appareil photo. De telles photos pourraient être utilisées pour contourner les contrôles de sécurité et commettre des tentatives d'effraction physique en vue de voler des serveurs, de l'équipement et des informations.

Dans des zones classifiées, un malfaiteur agissant de l'intérieur pourrait utiliser un téléphone cellulaire pour photographier des renseignements classifiés affichés à l'écran. Ces renseignements pourraient être utilisés par des agents de menace extérieure telle que le crime organisé afin de contrecarrer les projets et les enquêtes de l'ASFC ou éviter la perception des douanes et de l'accise.

Bien que ces exemples portent seulement sur les objectifs inopinés éventuels qui peuvent être la cible d'utilisation non autorisée de caméras ou d'appareils photos incorporés dans des appareils sans fil, ils montrent les menaces évidentes qui pèsent sur la technologie sans fil et essentiellement parce que ce type d'appareils sans fil continuera à être commercialisé avec des fonctions toujours croissantes.







## Casques d'écoute

Les utilisateurs portent de plus en plus des casques d'écoute sans fil lorsqu'ils conduisent. Plusieurs modèles utilisent les ondes radio et les signaux infrarouges. Les émissions des casques d'écoute telles que les conversations téléphoniques et les enregistrements numériques (enregistrements sonores) sont transmises au casque d'écoute dans l'air par l'appareil sans fil (téléphone cellulaire, PDA, ordinateur portatif, etc.).

De nombreuses organisations et gouvernements étrangers font de plus en plus couramment de l'espionnage industriel (vol des secrets d'une organisation). Utilisant une variante du « war driving », (détecteur d'accès) les adversaires procèdent à des écoutes électroniques de conversations et d'informations non codées de cadres supérieurs en les suivant dans leurs voitures. Des personnes malveillantes compétentes telles que celles des services de renseignements étrangers et du crime organisé peuvent aussi intercepter et même déchiffrer les conversations sur téléphone cellulaire encodées.



# 8. Utilisation des technologies et appareils sans fil à l'ASFC

Les appareils sans fil sont des outils précieux utilisés en fonction des besoins commerciaux et opérationnels. Les appareils, systèmes et services sans fil sont autorisés dans le cadre du travail à condition de s'en servir conformément aux présentes lignes directrices et aux politiques de l'ASFC.

Veuillez-vous souvenir des généralités suivantes :

- La transmission de renseignements Protégé B doit être encodée et protégée au moyen d'une signature numérique et d'un cryptage approuvés par l'ASFC.
- Les renseignements Classifié ou Protégé C ne doivent jamais être créés, stockés ou transmis à l'aide de technologies sans fil sans avoir complété le processus de certification et d'accréditation en consultation avec la Direction générale de la sécurité et des normes







professionnelles (DSNP) et la DSCTI. Les renseignements Classifié ou Protégé C exigent une protection plus rigoureuse devant être autorisée et approuvée par la DSNP.

- Les appareils sans fil appartenant à des individus, soit les appareils qui n'ont pas été fournis ni autorisé par l'ASFC, ne devraient pas être utilisés pour exercer des activités de l'ASFC ni être utilisés dans les locaux de l'ASFC.

Actuellement, un certain nombre de services et d'appareils sans fil peuvent être utilisés dans les locaux de l'ASFC.

Lorsque les appareils, les systèmes et les services sans fil non autorisés sont nécessaires pour répondre aux exigences d'affaires, la Division de la sécurité et de la continuité de la TI en collaboration avec les intervenants de la DSIST et avec la Direction de la sécurité et des normes professionnelles peuvent les autoriser au cas par cas et en fonction des résultats d'une évaluation des risques de la TI et si nécessaire, l'instauration de mesures de sécurité supplémentaires.

## Bluetooth

L'utilisation des écouteurs Bluetooth est autorisée avec les appareils portables BlackBerry de l'ASFC. Pour des précisions sur la façon d'activer le Bluetooth sur les appareils BlackBerry, veuillez consulter le site de l'ARC concernant l'utilisation du courriel sur les appareils sans fil de l'ARC.

Pour tout renseignement complémentaire, veuillez consulter les Directives sur la façon d'activer le Bluetooth BB.

## Équipement périphérique

### Casques d'écoute sans fil connectés aux téléphones cellulaires (à bord de véhicules)

Dans certaines provinces, la loi interdisant l'utilisation de téléphones cellulaires en conduisant un véhicule a été adoptée. Un écouteur câblé peut être utilisé dans un véhicule afin d'obtenir la connexion. En outre, un écouteur Bluetooth ou une trousse pour la voiture peut être utilisé. Pour obtenir des précisions concernant l'utilisation approuvée de l'équipement sans fil pour les BB, veuillez consulter le site de l'ARC sur le courriel sur les appareils sans fil (BlackBerry).

### Téléphones cellulaires, équipement de télécommunication par satellite ou téléphones sans fil

Les téléphones cellulaires, ainsi que l'équipement de communication par satellite et les téléphones sans fil, peuvent être utilisés pour le stockage, l'extraction et la transmission d'informations non délicate par messagerie vocale. Cependant, l'extraction de messages reçus dans la boîte aux lettres électronique au bureau exigeant l'utilisation d'un mot de passe, d'un code d'accès ou d'un NIP n'est pas autorisée. Ces contrôles d'authentification sont considérés de nature délicate et peuvent être facilement interceptés et compromis.







Les téléphones cellulaires, ainsi que l'équipement de communication par satellite et les téléphones sans fil, ne peuvent pas être utilisés pour le stockage, l'extraction et la transmission de voix ou de données Protégé A, B ou C, notamment l'extraction de messages reçus dans la boîte aux lettres électronique au bureau. En plus, les téléphones cellulaires ne doivent pas être utilisés pour explorer Internet ou y accéder (c.-à-d., une connexion à un fournisseur d'accès Internet [FSI]). Les téléphones cellulaires ne doivent pas être utilisés pour saisir des images (filmes ou fixes) ou faire des enregistrements sonores. La messagerie textuelle n'est permise que sur autorisation explicite de l'ASFC.

## Téléavertisseurs

Les téléavertisseurs peuvent seulement être utilisés pour le stockage, l'extraction et la transmission d'informations non confidentielles.

## Appareils portables BlackBerry (BB) approuvés par l'Agence

Le BlackBerry est un appareil sans fil qui permet aux utilisateurs autorisés de l'ASFC de recevoir et d'envoyer des courriels. Les appareils BB fournis par l'ASFC permettent aux utilisateurs de stocker, d'extraire et de transmettre des courriels ayant une cote allant jusqu'à Protégé B pour les communications dans le système interne de l'ASFC. Les services d'ICP sont activés et ils permettent aux utilisateurs de crypter des courriels et d'envoyer des messages par courriel sécurisé. En plus de la fonctionnalité des courriels, les services suivants sont autorisés : SMS (messages textes), NIP-à-NIP ; les communications vocales et les fonctionnalités des caméras numériques.. Les SMS, les messages NIP-à-NIP et les communications vocales sur les appareils BB ne sont pas sécurisés; par conséquent, les messages textes et les conversations téléphoniques doivent se limiter aux renseignements de nature non délicate.

La saisie de photos par caméra numérique (image fixe ou vidéo animée) ne doit pas servir pour des photos de nature délicate comme des configurations de réseau, des locaux ou des employés de l'ASFC. Les photos qui sont considérées comme étant inappropriées, offensantes ou illégales ou les photos qui pourraient donner une image négative de l'Agence ne doivent pas être prises.

Pour obtenir des précisions supplémentaires à ce sujet, veuillez consulter le site de l'ARC concernant l'utilisation du courriel sans fil. Pour l'ASFC, veuillez-vous rendre à la section intitulée « processus d'approbation de l'ASFC ». Veuillez consulter le site de l'ARC pour obtenir une liste complète des lignes directrices pour les utilisateurs et des services approuvés pour les BlackBerry.

## Ordinateurs portatifs

Les services d'accès sécurisé à distance (ASD) sans fil de l'ASFC sur les ordinateurs portatifs fournis par l'ASFC sont approuvés. Pour obtenir des précisions à ce sujet, veuillez consulter le site de l'ARC sur l'accès à distance sécurisé.

## Dispositifs de pointage sans fil

L'utilisation de dispositifs de pointage sans fil comme ceux de pointage laser est autorisée.







## Claviers sans fil

Les claviers sans fil ne sont pas autorisés.

## Autres appareils dotés de dispositifs d'enregistrement d'images ou de conversations

L'utilisation de tous les autres appareils qui ne sont pas compris dans les présentes lignes directrices sur l'utilisation des technologies et appareils sans fil, ainsi que dans la politique connexe, et qui sont dotés d'appareil photo numérique, de microphone ou de fonctions d'enregistrement n'est pas autorisée dans les locaux de l'Agence.

Note : Toute question concernant les téléphones cellulaires, l'équipement de communication par satellite et autres appareils de communications ne dépendant pas du système TI doit être adressée à la Division des contrats, des biens et des télécommunications, de la Direction générale du contrôle.

# 9. Mesures de sécurité des utilisateurs - menaces courantes touchant les sans fil

La présente partie comprend des mesures de sécurité additionnelles que vous pouvez appliquer contre les menaces aux appareils sans fil courants.

1. Connaître le degré de sensibilité des renseignements dans vos communications sans fil. Ne discutez pas de renseignements Classifié ou Protégé C dans vos conversations au téléphone cellulaire et ne les stockez pas dans ces téléphones, dans des PDA et dans des ordinateurs portatifs. Communiquez avec la Direction de la sécurité et des normes professionnelles pour des renseignements sur l'information classifiée.
2. Ne changez pas vos paramètres de sécurité. Les paramètres de sécurité établis dans les ordinateurs portatifs et les PDA sont correctement configurés pour la sécurité quand ils vous sont livrés.
3. Ne téléchargez pas des logiciels dans les téléphones cellulaires, les PDA et les ordinateurs portatifs. Les logiciels téléchargés peuvent contenir un programme malveillant, notamment des sonneries, des partages de fichiers (comme Kazaa) et d'autres applications personnalisables.
4. N'affichez pas votre numéro de téléphone cellulaire ni votre adresse électronique. Les pirates informatiques visitent les sites Web pour y recueillir des adresses électroniques et des numéros de téléphone cellulaire. En limitant le nombre de personnes qui ont vos coordonnées, vous limitez le pourriel et le risque d'être victime de ces pirates.
5. Ne visitez pas les liens indiqués dans des courriels ou des messages textes. Méfiez-vous des adresses URL envoyées dans





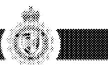
des courriels ou des messages textes non sollicités. Des liens qui semblent légitimes peuvent conduire à des sites Web malveillants.
6. Sécurité physique au bureau. Quand vous sortez de votre bureau, enfermez tous les ordinateurs portatifs, les PDA et les appareils sans fil. Les mettre hors de vue.
7. Sécurité physique lors des déplacements. Quand vous êtes dans des endroits publics, surveillez vos téléphones cellulaires, vos ordinateurs portatifs et vos PDA. Ne les enregistrez pas comme des bagages en soute. Mettez-les dans des bagages qui ne ressemblent pas à des étuis d'ordinateur portatif.
8. Chiffrer vos données. En cas de vol de votre appareil sans fil, les voleurs ne pourront pas lire vos données. Les disques durs des ordinateurs portatifs approuvés par l'ASFC sont chiffrés. Si vous ne conservez pas de données dans les appareils sans fil mais dans des clés USB, utilisez seulement celles qui peuvent être chiffrées.
9. Utilisez des mots de passe rigoureux. Sélectionnez des mots de passe difficiles à deviner et composés d'au moins huit caractères parmi lesquels on trouve un chiffre, une lettre en majuscule, une lettre en minuscule et un caractère spécial (#, !, &).
10. Signalez immédiatement le vol ou la perte d'appareils sans fil.
    - Signalez la perte ou le vol d'appareils sans fil à votre service des TI afin que ce service désactive l'appareil du réseau sans fil.
    - Vous devez aussi informer votre supérieur et dans le cas d'un incident de sécurité informez aussi la Direction de la sécurité et des normes professionnelles.

# 10. Signalement des incidents relatifs à la sécurité des TI

Tout incident de sécurité des TI concernant du courriel doit être signalé immédiatement. Pour plus de renseignements sur la notification d'un incident de sécurité, consultez : « Comment rapporter les incidents de sécurité », dans la section de la Direction de la sécurité et des normes professionnelles d'Atlas.

Un incident de sécurité signifie qu'il y a eu, par exemple :

- Compromission soupçonnée ou réelle de renseignements protégés ou classifiés.
- Envoi de programmes malveillants ou alertes / attaques virales contre les systèmes informatiques ou de communication de l'ASFC ou autres circonstances menant à la dégradation du fonctionnement du système (ne transférez pas des fichiers ou des messages si vous pensez que votre ordinateur est infecté, appelez le service de dépannage de TI).
- La perte, le vol, la compromission ou la destruction de renseignements, d'appareils sans fil, de systèmes ou de services ou d'autres biens appartenant à l'ASFC ou sous le soin de celle-ci.
- Les incidents liés à la technologie sans fil, soupçonnés de constituer des infractions inacceptables, illégales ou criminelles.



- Les incidents liés à la technologie sans fil ayant une incidence sur les opérations gouvernementales ou qui pourrait susciter une révision des normes opérationnelles ou de la documentation technique.

# 11. Sommaire

Puisque les technologies sans fil évoluent rapidement, l'Agence continuera à évaluer des solutions sans fil sécuritaires pour l'ASFC. Les présentes lignes directrices seront mises à jour pour refléter les changements technologiques et les mesures de sécurité connexes pour protéger les solutions de la technologie sans fil adaptées par l'Agence.

# 12. Demande de renseignements

Le présent document a été rédigé à l'intention de l'ASFC par la Division de la sécurité et de la continuité de la TI, Direction générale de l'information, des sciences et de la technologie en collaboration avec la Direction de la sécurité et des normes professionnelles, Direction générale du contrôle.

Adresser toute observation concernant le présent document à la sécurité des TI de l'ASFC :
Courriel : CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca et l'Intranet

# 13. Abréviations

| | |
|---|---|
| 1G | Première génération (téléphones cellulaires) |
| 3G | Troisième génération |
| CST | Centre de la sécurité des télécommunications du Canada |
| IEEE | Institut des ingénieurs électriciens et électroniciens |
| IR | Infrarouge |
| IrDA | *Infrared Data Association* |
| MB | Haut débit mobile |
| MBWA | Accès à large bande sans fil mobile |
| RF | Radio fréquence |







| | |
|---|---|
| WiFi | Technologie Wi-Fi |
| WLAN | Réseau local sans fil |
| WMAN | Réseau métropolitain |
| WMAX | *Wireless Interoperability for Microwave Access* |
| WPAN | Réseau personnel sans fil |
| WWAN | Réseau étendul sans fil |

## 14. Définitions

| Terme | Definition |
|---|---|
| 1G | 1G est la première génération de téléphones cellulaires et est analogue |
| 3G | 3G est la troisième génération de normes de technologies de téléphones cellulaires, remplaçant 2G et avant 4G. Elle s'appuie sur la norme de l'Union internationale des télécommunications (UIT). Les réseaux 3G de téléphonie cellulaire sont étendus et ont évolué pour incorporer des accès Internet à haute vitesse et la visiophonie. |
| Bluetooth | Technologie radio-courte distance destinée à simplifier la transmission de données sur de courtes distances entre les appareils fixes et les appareils cellulaires créant des réseaux personnels sans fil (PAN). |
| IEEE 802.11 | Ensemble de normes relatives à la télématique de réseau local sans fil (WLAN) élaborées par le Comité de normalisation LAN/MAN de l'IEEE (IEEE 802) sur les bandes du spectre publiques de 5 GHz et de 2,4 GHz. Les réseaux de IEEE 802.11 sont des réseaux haut débit à faible portée développés principalement pour les données. |
| Infrarouge | Le rayonnement infrarouge (IR) est un rayonnement électromagnétique d'une longueur d'onde supérieure à celle de la lumière visible mais plus courte que celles de la bande de |







| | |
|---|---|
| | fréquence des téraherzt et des micro-ondes. |
| IrDA | Dans la technologie de l'information et des communications, IrDA est le sigle de *Infrared Data Association*, une norme de communication entre des appareils (ordinateurs, PDA et téléphones cellulaires) sur des courtes distances à l'aide de signaux infrarouges. |
| Hameçonnage | Usurpation d'identité d'une personne ou d'un organisme de confiance dans le but de voler les renseignements personnels d'un individu, généralement dans un dessein de vol d'identité. Par exemple, un message électronique peut sembler provenir d'une banque bien connue et demander aux destinataires de visiter un site Web afin de confirmer les détails de leur compte, mais le site Web est en fait contrôlé par un parti hostile. |
| WiFi | Nom de marque de la technologie populaire sans fil [802.11) utilisée dans les réseaux familiaux, les téléphones cellulaires, les jeux vidéo, etc. |
| WiMAX | WiMAX, acronyme pour *Worldwide Interoperability for Microwave Access*, est une technologie de télécommunications qui assure la transmission des données de plusieurs façons, allant de liaisons point à point à l'accès aux services de type cellulaire. Cette technologie fondée sur les normes permet l'accès au dernier kilomètre à large bande comme solution de rechange au câble et DSL. |
| Réseau local sans fil | Le LAN ou WLAN est un réseau local sans fil qui connecte sans utiliser des fils deux ordinateurs ou appareils ou plus. |
| Réseau métropolitain sans fil | Les réseaux métropolitains sans fil (WMAN) sont des réseaux sans fil qui connectent plusieurs LAN sans fil. WiMAX est le terme utilisé en référence aux WMAN et est décrit dans *IEEE 802.16d/802.16e*. |
| Réseau personnel sans fil | WPAN désigne un réseau personnel à très faible portée, habituellement de quelques mètres. Ce réseau peut servir aux communications entre les appareils personnels (communications interpersonnelles) ou pour relier un réseau de haut niveau à Internet (une liaison montante). . |
| Large bande mobile | Cette expression décrit divers types d'accès Internet haute vitesse sans fil à l'aide d'un modem portatif, d'un téléphone ou d'un autre appareil. Différentes normes de réseau peuvent |







| | |
|---|---|
| | être utilisées (WiMAX, UMTS/HSPA, EV-DO et quelques systèmes satellitaires portatifs). |
| Accès à large bande sans fil mobile | Se reporter à la définition de "Large bande mobile" ci-dessus. Le 11 décembre 2002, le Comité de normalisation de l'IEEE a approuvé la mise sur pied de l'IEEE 802.20, groupe de travail sur l'accès à large bande sans fil, dont l'objectif est l'élaboration de la spécification d'une interface hertzienne à base de paquets efficace et optimisée pour le transport des services IP. Le but étant d'assurer le déploiement dans le monde de réseaux d'accès à large bande sans fil mobiles, multiconstructeurs, compatibles, à un coût abordable, omniprésents, toujours en service et répondant à la demande des utilisateurs commerciaux et résidentiels. |
| Réseau étendu sans fil | WWAN, acronyme de *Wireless Wide Area Network*, est un réseau étendu sans fil différent du WLAN (réseau local sans fil LAN) car il utilise des technologies de réseau cellulaire comme WIMAX |

# 15. Références et lectures complémentaires

* Pour accéder à ces sites, vous devez utiliser un ordinateur avec un accès Internet.

ARC - Norme relative à la sécurité du réseau sans fil (2005)
CSTC: ITSB-49 Enregistreurs de frappe et logiciels espions (Mai 2008) *
CSTC: ITSPSR17a Évaluation des vulnérabilités de Bluetooth Juin 2008) *
NIST SP800-124 Guidelines on Cellular Phone and PDA Security (Juillet 2008) * Seulement disponible en anglais
NIST SP800-121 Guide to Bluetooth Technology (Juillet 2008) * Seulement disponible en anglais
NSA: Bluetooth Security (Déc 2009) * Seulement disponible en anglais
NSA: So your boss bought you a new laptop... How do you Identify and disable wireless capabilities? (Mai 2007) * Seulement disponible en anglais
Sécurité publique Canada : Pratiques modèles générales à l'égard de la sécurité des ordinateurs portables (13 févr. 2008) *
ARC: Solution de courriel sans fil - Politique d'utilisation (28 nov., 2007)
ARC: BlackBerry Operations Guide (23 juillet 2007) Seulement disponible en anglais.
ASFC : Politique de téléphones cellulaires (1er avril 2008)



Blackberry: Security Technical Overview Blackberry Devices with Bluetooth Technology (18 juin 2008) * Seulement disponible en anglais
USCERT: Cybersecurity for Electronic Devices (20 août 2008) * Seulement disponible en anglais
USCERT: Defending Cellular Phones and PDAs against attack (9 août 2008) * Seulement disponible en anglais
USCERT: Protecting Portable Devices Data Security (10 oct. 2007) * Seulement disponible en anglais
ARC : Guide de l'utilisateur - Services mobiles sans fil de Telus (v1.0) *
CSEC - CSTC - Sécurité de la messagerie BlackBerry NIP à NIP *

* Pour accéder à ce site, vous devez utiliser un ordinateur raccordé à Internet.

# Annexe A - Mesures de protection des appareils mobiles sans fil

## Au bureau

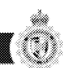
1. Gardez tous les appareils sans fil dans un bureau fermé ou les enfermez dans des tiroirs d'un bureau ou tout autre endroit pouvant être verrouillé. Si les appareils ne sont pas surveillés, les mettre en mode de verrouillage en utilisant le code approprié (s'assurer que l'ordinateur portable est verrouillé à la station d'accueil ou que le PDA est enfermé dans un tiroir.)
2. Une porte verrouillée n'est pas une protection suffisante. Il faut, comme pour tout objet de valeur, les mettre dans un endroit sûr du bureau quand vous n'y êtes pas.

## En déplacement

1. Ne laissez jamais seuls les appareils mobiles sans fil dans des endroits où vous risquez de les oublier et où quelqu'un peut les prendre. Aux points de contrôle de sécurité des aéroports, attendez que l'on vous invite à passer la barrière de sécurité à détecteur de métaux avant de poser les appareils sur le tapis roulant de l'appareil de détection.
2. Ne prêtez pas votre appareil mobile sans fil à un inconnu.
3. N'installez pas de logiciel de partage de fichiers (comme Kazaa, Limewire, etc.) ou tout autre logiciel non autorisé dans des appareils mobiles sans fil.
4. Ne conservez ni mots de passe ni numéros de compte dans des appareils mobiles sans fil et ne les communiquez à personne.
5. Pour donner le change, transportez les ordinateurs portables ou tout autre appareil mobile sans fil dans un étui ou une sacoche générique.

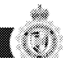






6. N'enregistrez jamais votre ordinateur portable ou tout autre appareil mobile sans fil comme bagage en soute chez un transporteur commercial (aérien, ferroviaire, etc.), ne les remettez pas à des chasseurs d'hôtel et ne les laissez pas dans des consignes à bagages d'hôtels.
7. Ne mettez jamais les ordinateurs portables ou tout autre appareil mobile sans fil dans le coffre d'un taxi ou le compartiment à bagages d'une limousine ou d'une navette.
8. Verrouillez votre ordinateur portable ou tout autre appareil mobile sans fil dans le coffre des voitures louées, mais si vous quittez la voiture pour une période relativement longue ou durant toute la nuit, mettez-les dans votre chambre ou transportez-les avec vous.
9. Si vous ne pouvez pas transporter l'appareil mobile sans fil, mettez-le dans le coffre-fort de l'hôtel ou de la chambre.
10. N'oubliez pas que n'importe qui peut intercepter des communications sans fil. Il n'est pas nécessaire de brancher quel que fil que ce soit.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Addendum to CBSA's IT Security Policy on the Use of Wireless Technology

## Use of PIN-to-PIN messaging on BlackBerry Devices

PROTECTION • SERVICE • INTEGRITY

Canada



# Introduction

This addendum will focus on threats to the security of data transmission related specifically to PIN-to-PIN communications on BlackBerry devices.[1]

# Background

BlackBerry PIN-to-PIN (sometimes referred to as Peer-to-Peer) messaging is similar to e-mail in that it allows BlackBerry device users to send messages to each other. There are however two main differences:

1. Messages are addressed to a PIN (personal identification number) instead of an e-mail address. The PIN is a hardware address that is associated with the device, it is not an authentication password nor is it a user identifier.
2. Users who know the PINs of other users' BlackBerry devices can use them to directly exchange data messages with the other devices across the wireless network (outside of the Agency e-mail system), thus bypassing the internal e-mail servers and security filters.

# PIN-to-PIN Security Issues

PIN-to-PIN messaging is useful for emergency communications in situations where the Agency email servers are down. However, if the wireless carrier's cellular network is down, the PIN-to-PIN messaging will also be unavailable.

PIN-to-PIN messaging suffers from several important security vulnerabilities that users should be aware of:

## 1. PIN-to-PIN transmission security

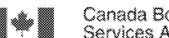
PIN-to-PIN is not suitable for exchanging sensitive messages (all Protected and Classified information). The encryption key used is a global cryptographic key that is common to every BlackBerry device. This means any BlackBerry device can potentially decrypt all PIN-to-PIN messages, or unfriendly third parties could intercept the messages over the air and easily decrypt them.

## 2. PIN Address Vulnerability

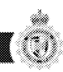
A BlackBerry device that has been used for PIN messaging should not be recycled for re-use. The hard-coded PIN cannot be erased or modified therefore the PIN does not follow a user to a new device. Even after memory wiping and resetting the device, the











BlackBerry still has the same PIN identity and will continue to receive PIN messages addressed to that PIN. This can expose unsuspecting users of BlackBerry devices to potential information compromises, such as viewing messages sent to the wrong recipient (the PIN is a device ID and not a user ID) or impersonation (a known PIN credential might be mistakenly accepted as being from the previous owner).

## 3. Bypass of Virus / Malware Scanning and Spam Filtering mechanisms

PIN-to-PIN messaging bypasses the Agency e-mail security filters. Users may become vulnerable to viruses and malware code as well as spam messages if their PIN becomes known to unauthorized individuals.

## 4. Message Content Logging and Audit Trail

The Agency is required to retain and store messages that constitute records, including those sent or received on wireless devices, for ATIP and audit purposes.

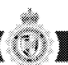
Messages identified as corporate information must be retained. Corporate information is information recorded in any form, created or received by an organization or person conducting official business.

Messages identified as containing transitory information should be deleted when it is no longer of use. The exception of when not to delete messages containing transitory information is after receiving a formal request under the *Access to Information Act* (ATIP) or *Privacy Act* relating to that information. Transitory information is information that is required only for a limited time to ensure a routine action is completed or a subsequent record is prepared.

For further details regarding Corporate and Transitory Information refer to Annex A of the Policy on the Appropriate Use of E-mail.

## 5. PIN is Identifiable

Although the body of a message may be secure, the PIN itself is still transmitted in the clear. If the identity of an individual can be associated with their assigned PIN, an adversary may be able to use this information for targeting purposes.



## Recommendations

PIN number assignments are considered personal information and should be kept separate from phone / e-mail lists, and never be disclosed or released to unauthorized individuals. Users should not publish their PIN, such as in e-mail messages.

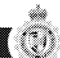
Since the BlackBerry uses a global encryption key, do not transmit any sensitive information.

PINs are associated with the physical device and not a specific user. As a user of a BlackBerry device which has been used for PIN messaging, ensure that the device is destroyed and not recycled.

---

[1] The content of this addendum is based on the Communications Security Establishment Canada's (CSEC) IT Security Bulletin, ITSB-57, pertaining to the Security of BlackBerry PIN-to-PIN messaging.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Addenda à la politique de sécurité des TI de l'ASFC concernant l'utilisation de la technologie sans fil

## Utilisation de la messagerie NIP à NIP sur les appareils BlackBerry



# Introduction

Le présent addenda porte sur la menace que représentent les communications NIP à NIP des appareils BlackBerry pour la sécurité des transmissions des données.[1]

# Contexte

La messagerie NIP à NIP du BlackBerry (aussi appelée personne à personne) est semblable au courriel car elle permet aux utilisateurs du BlackBerry de s'envoyer des messages entre eux. Il y a cependant deux différences majeures à souligner.

1. Les messages sont envoyés à un NIP (numéro d'identification personnel), et non à une adresse électronique. Le NIP est une adresse matérielle associée à l'appareil et non un mot de passe d'authentification ou un identificateur d'utilisateur.
2. Les utilisateurs qui connaissent les NIP d'autres appareils BlackBerry peuvent s'en servir pour échanger directement des messages avec d'autres appareils en passant par le réseau sans fil (hors du système de courrier électronique de l'Agence), contournant ainsi les serveurs internes de courrier électronique et les filtres de sécurité.

# Questions de sécurité relatives au NIP à NIP

La messagerie NIP à NIP est utile pour les communications d'urgence, lorsque les serveurs de courrier électronique de l'Agence ne fonctionnent pas. Cependant, si le réseau de téléphonie mobile de l'appareil est inactif, la messagerie NIP à NIP le sera également.

La messagerie NIP à NIP possède plusieurs vulnérabilités majeures en matière de sécurité, dont les utilisateurs devraient être conscients.

## 1. Sécurité des transmissions faites avec le NIP à NIP

Le NIP à NIP ne convient pas à l'échange de messages de nature délicate (toute information protégée ou classifiée). La clé de chiffrement utilisée est une clé cryptographique globale, partagée par chaque appareil BlackBerry, ce qui veut dire que n'importe quel BlackBerry peut déchiffrer les messages NIP à NIP, ou qu'un tiers parti inamical peut intercepter les messages et facilement les déchiffrer.

## 2. Vulnérabilités de l'adresse NIP

Un appareil BlackBerry qui a servi à envoyer un message NIP à NIP ne doit pas être recyclé ou être réutilisé. Le NIP incorporé à l'appareil ne peut être effacé ou modifié ce qui veut dire qu'il ne suit pas l'utilisateur lorsque celui-ci change d'appareil BlackBerry. Même après avoir effacé la mémoire et réinitialiser l'appareil, le BlackBerry conserve le même NIP et continuera à recevoir des messages NIP à NIP adressés à ce NIP. Les utilisateurs non méfiants peuvent donc être plus vulnérables à d'éventuelles situations où l'information serait compromise, comme voir des messages destinés à une autre personne (le NIP est propre à l'appareil et non à l'utilisateur) ou usurper l'identité d'une personne (un justificatif d'identité de NIP connu pourrait être accepté par erreur comme étant celui de l'ancien utilisateur).

## 3. Passer outre les mécanismes de logiciels antivirus et contre les programmes malveillants ainsi que ceux de filtrage de pourriel

La messagerie NIP à NIP contourne les filtres de sécurité du courrier électronique de l'Agence. Les utilisateurs peuvent être vulnérables face aux virus et aux codes malveillants ou au pourriels si des personnes non autorisées viennent à connaître leurs NIP.

## 4. Traces du contenu, de la consignation et de la vérification des messages

L'Agence est tenue de conserver et d'entreposer les messages qui constituent des dossiers, dont ceux envoyés ou reçus sur des appareils sans fil, à des fins d'AIPRP et de vérification.

Un message identifié comme étant de l'information organisationnelle doit être conservé. Une information organisationnelle est toute information enregistrée sous diverses formes, créée et reçue par une organisation ou une personne pour exécuter des fonctions officielles.

Un message comportant de l'information transitoire devrait être supprimé lorsqu'il n'est plus utile. Toutefois, ces messages ne doivent pas être supprimés après avoir reçu une demande officielle en vertu de la *Loi sur l'accès à l'information* ou *la Loi sur la protection des renseignements personnels* reliée à cette information (AIPRP). Une information transitoire est toute



information requise uniquement pour un temps limité pour s'assurer qu'une activité de routine est exécutée ou qu'un document subséquent est préparé.

Pour de plus amples renseignements sur l'information organisationnelle ou transitoire, veuillez consulter l'annexe A de la Politique sur l'utilisation appropriée du courrier électronique.

## 5. NIP identifiable

Bien que le corps du message soit protégé, le NIP lui-même est tout de même transmis à découvert. Si l'identité d'une personne peut être associée à son NIP, un adversaire pourrait être en mesure d'utiliser cette information à des fins de ciblage.

# Recommandations

Le NIP est considéré comme une information personnelle et ne devrait pas être inscrit dans une liste de coordonnées au même titre que le numéro de téléphone ou l'adresse électronique. Il ne devrait également jamais être divulgué à des personnes non autorisées. Les utilisateurs ne devraient pas diffuser leurs NIP, entre autres dans un courriel.

Puisque le BlackBerry se sert d'une clé cryptographique globale, ne transmettez aucun renseignement de nature délicate.

Les NIP se rattachent à l'appareil et non à l'utilisateur. À titre d'utilisateur d'un BlackBerry qui a servi à envoyer des messages NIP à NIP, assurez-vous que l'appareil est détruit et non recyclé après utilisation.

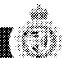
---

[1] Le contenu du présent addenda se base sur le Bulletin de sécurité des TI, ITSB-57, du Centre de la sécurité des télécommunications Canada (CSTC) qui traite de la sécurité de la messagerie NIP à NIP du BlackBerry.





Canada Border Services Agency    Agence des services frontaliers du Canada



# Appendix to CBSA's IT Security Policy on the Use of Wireless Technology

# Additional Security Requirements for Wireless Devices

PROTECTION • SERVICE • INTÉGRITÉ

Canada



## Introduction

This appendix provides additional security requirements in support of the Policy on the Use of Wireless Technology as well as further guidance to protect the sensitive information saved, processed and transmitted on wireless devices.

## Context

Wireless devices include all PDA's (such as the BlackBerry), cellular phones, smart phones, laptops or any other device that has the capability to store, process, transmit or share information, whether the device has audio, analog/digital and/or image capture functionality.

## Wireless Devices with voice transmission capability

Voice transmission capability must be disabled when attending a meeting at which sensitive information up to and including Protected B is being shared (applies to all wireless devices that have the same capabilities). For guidance on the handling of information above Protected B, contact the Security and Professional Standards Directorate.

## Mitigation strategy

For meetings where sensitive information up to and including Protected B is being shared:

- Use a BlackBerry Microphone Security Plug; and/or
- Power off the device and leave it outside of the meeting room.

## SMS and PIN-to-PIN functionality

Short Message Service (SMS) has been enabled on CBSA approved Blackberry devices

SMS and PIN-to-PIN are never to be used for communicating or storing sensitive, corporate information. SMS and PIN-to-PIN are not suitable for exchanging sensitive messages (All Protected and Classified information). Only transitory information, information that is required only for a limited time to ensure a routine action is completed, is to be communicated.

## Additional Requirements for Wireless Devices

1. Do not download unauthorized software such as ringtones, file-sharing or any applications that provide additional wireless functionality, etc.;
2. Ensure that your business contact information (such as your work cellular phone number, BlackBerry PIN number and/or e-mail address) is only posted on authorized websites for approved CBSA



business purposes (i.e., do not post them on unauthorized blogs or social networking sites);

3. Ensure that CBSA information on wireless devices in public areas can not be observed such as shoulder surfing of laptops;
4. Ensure that CBSA information on wireless devices is not stolen and observe physical security when travelling (such as ensuring CBSA wireless devices in your possession are carried in inconspicuous luggage or carrying cases, not checked as baggage, not loaned to strangers or other unauthorized users, and not left unattended in public areas);
5. Do not discuss sensitive information or transmit text messages (i.e. SMS or PIN-to-PIN) that contain CBSA corporate and sensitive information;
6. Do not change the configuration or security settings of any CBSA wireless device in your possession; and
7. Immediately report lost or stolen wireless devices to your supervisor as well as the local Security officer. For BlackBerry devices, also immediately contact CRA at the following link in order to have the device deactivated from the wireless network. http://infozone/english/r2423153/dtim_gidt/nsd/wire/index/thftLss-e.asp
   CBSA security emergency procedures are available here

For more information on "Reporting Security Incidents" please refer to Chapter 15 of the CBSA Security Volume

## Use of the BlackBerry Microphone Security Plug

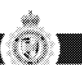
The BlackBerry Microphone Security Plug (hereinafter referred to as the Security Plug) is a small hardware device which is inserted into the headset jack of a BlackBerry, disabling the microphone

Its intended use is to prevent conversations being overheard electronically, where the information is up to and including Protected B, in accordance with the CBSA Policy and Guidelines on the Use of Wireless Technology. The security plug is similar to a headset where the voice communication is transmitted.

### To activate the security plug

- Connect the security plug into the headset jack of the BlackBerry
- The security plug must be inserted fully into the jack so that its base is flush with the side of the BlackBerry
- An LED indicator on the security plug is illuminated indicating that the plug is functioning properly.
- The security plug blocks voice communications.

### Disabling the ring tone



- Although the security plug ensures that there is no voice recognition, it does not block the ring tone.
- The user must manually change the ring tone to either vibrate or mute.

## Answering a call

- If a user needs to answer a call, the user needs only to remove the security plug.
- Voice communications are enabled by removing the security plug from the BlackBerry headset jack.

## Regular testing (for functionality)

- The plug and the BlackBerry device should be tested regularly to ensure proper functionality (attempt a voice call, watch for LED and check that no audio is transferred when a call connects).
- Broken solder connections inside the BlackBerry can result in the plug not working.

## Procurement

- Contact your local IT help desk to obtain/purchase a Security Plug.

Agence des services frontaliers du Canada | Canada Border Services Agency



# Annexe à la politique de l'ASFC sur la sécurité des TI concernant l'utilisation de la technologie sans fil

# Exigences supplémentaires en matière de sécurité pour les appareils sans fil

PROTECTION • SERVICE • INTÉGRITÉ





## Introduction

Cette annexe présente les exigences supplémentaires en matière de sécurité à l'appui de la politique concernant l'utilisation de la technologie sans fil. Elle offre aussi des directives sur la protection de l'information délicate enregistrée, traitée et communiquée à l'aide d'appareils sans fil.

## Contexte

Les appareils sans fil comprennent les assistants numériques (notamment le BlackBerry), les téléphones cellulaires, les téléphones intelligents, les ordinateurs portatifs ou tout autre appareil capable de stocker, de traiter, de communiquer ou d'échanger de l'information, peu importe s'il possède une fonctionnalité audio ou analogique/numérique ou une fonctionnalité de saisie d'image.

## Dispositifs sans fil avec fonction de transmission de la voix

La fonction de transmission de la voix doit être désactivée lors d'une réunion où est échangée de l'information délicate allant jusqu'au niveau Protégé B inclusivement (s'applique à tout appareil sans fil ayant cette fonction). Pour obtenir des directives sur le traitement de l'information de niveau supérieur au niveau Protégé B, communiquez avec la Direction de la sécurité et des normes professionnelles.

## Stratégie d'atténuation

Lors des réunions où est échangée de l'information de nature délicate allant jusqu'au niveau Protégé B inclusivement, veuillez :

- Utiliser le bouchon de sécurité pour appareils BlackBerry; et/ou
- Éteindre l'appareil et le laisser à l'extérieur de la salle de réunion.

## SMS et NIP à NIP

Le service d'envoi de messages courts (SMS) a été mis en service pour les appareils BlackBerry approuvés de l'ASFC.

Les fonctionnalités SMS et NIP à NIP ne doivent jamais être utilisées pour communiquer ou stocker de l'information délicate ou organisationnelle. Le SMS et le NIP à NIP ne sont pas convenables pour l'envoi de messages de nature délicate (contenant toute information classifiée ou protégée). Seule l'information transitoire peut être communiquée, soit l'information requise uniquement pour un temps limité pour s'assurer qu'une activité de routine est exécutée.

## Exigences supplémentaires pour les appareils sans fil





1. Ne téléchargez pas de logiciels non autorisés comme des sonneries, des applications de partage de fichiers ou toute application fournissant des fonctions supplémentaires pour appareil sans fil, etc.;
2. Assurez-vous que vos coordonnées au bureau (notamment votre numéro de téléphone cellulaire, votre NIP de BlackBerry et votre adresse électronique) sont seulement affichées sur les sites Web autorisés par l'ASFC (c. à-d. ne les diffusez pas sur des blogues non autorisés ou sur des sites de réseautage social);
3. Assurez-vous que l'information de l'ASFC contenue sur un appareil sans fil ne peut être vue lorsque vous êtes dans un endroit public, par exemple par-dessus votre épaule lorsque vous utilisez votre ordinateur portatif;
4. Assurez-vous que l'information de l'ASFC contenue sur un appareil sans fil ne peut être volée et respectez les règles de sécurité physique lors de vos déplacements (entre autres, transportez les appareils sans fil de l'ASFC en votre possession dans des bagages ou des étuis de transport qui passent inaperçus, ne les enregistrez pas comme bagage, ne les prêtez pas à des étrangers ou à des utilisateurs non autorisés, et ne les laissez pas sans surveillance dans un lieu public);
5. Ne discutez pas d'information délicate ou organisationnelle de l'ASFC et n'envoyez pas de messages textes (c.-à-d. SMS ou NIP à NIP) qui en contiennent;
6. Ne changez pas la configuration ou les paramètres de sécurité d'un appareil sans fil de l'ASFC en votre possession;
7. Signalez immédiatement toute perte ou tout vol d'appareil sans fil à votre superviseur ainsi qu'à l'agent de sécurité local. Pour les appareils BlackBerry, contactez aussi immédiatement l'ARC à l'adresse suivante pour que l'appareil soit désactivé du réseau sans fil:
   http://infozone/francais/r2423153/dtim_gidt/nsd/wire/index/thftLss-f.asp
   Les procédures de sécurité et d'urgence de l'ASFC sont disponibles ici.

Pour plus d'information sur la façon de signaler des incidents de sécurité, consultez le chapitre 15 du Volume de sécurité de l'ASFC

## Utilisation du bouchon de sécurité pour les appareils BlackBerry

Le bouchon de sécurité ("security plug") pour appareils BlackBerry est un petit périphérique qui s'insère dans la prise d'écouteurs d'un BlackBerry et qui désactive le microphone.

Conformément à la politique et les directives de l'ASFC concernant l'utilisation de la technologie sans fil, on utilise le bouchon pour empêcher les conversations portant sur de l'information allant jusqu'au niveau Protégé B inclusivement d'être écoutées au moyen de procédés



électroniques. Le bouchon de sécurité est semblable à un casque d'écoute : la communication vocale est transmise à l'appareil.

## Activer le bouchon de sécurité

- Le bouchon de sécurité doit être inséré dans la prise d'écouteurs du BlackBerry.
- Il doit être inséré au complet dans la prise de sorte que sa base s'aligne de justesse avec le côté du BlackBerry.
- Un voyant DEL s'allume sur le bouchon de sécurité lorsque celui ci fonctionne.
- Le bouchon de sécurité empêche la communication vocale.

## Désactiver la sonnerie

- Même si le bouchon de sécurité empêche la reconnaissance vocale, il ne désactive pas la sonnerie.
- L'utilisateur doit lui-même mettre l'appareil en mode vibration ou le rendre muet.

## Répondre à un appel

- Si un utilisateur doit répondre à un appel, il n'a qu'à retirer le bouchon de sécurité.
- La communication vocale redevient possible lorsque le bouchon de sécurité est retiré de la prise d'écouteurs du BlackBerry.

## Tester régulièrement le bouchon (pour en vérifier le bon fonctionnement)

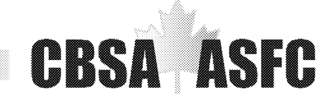
- Le bouchon et l'appareil BlackBerry devraient être testés régulièrement pour en vérifier le bon fonctionnement (tentez de passer un appel, faites attention au voyant DEL et vérifiez qu'aucun son n'est transmis lors d'une liaison téléphonique).
- Des joints de soudures brisés à l'intérieur de l'appareil BlackBerry peuvent faire en sorte que le bouchon ne fonctionne pas.

## Obtenir une fiche de sécurité

- Veuillez communiquer avec le bureau d'aide local de la TI pour obtenir ou acheter un bouchon de sécurité.








# POLICY ON EMERGENCY MANAGEMENT

## 1. *Preamble*

In accordance with the *Emergency Management Act* (EMA), Subsection 6.(1) and 6.(2), the Canada Border Services Agency (CBSA) is responsible for the prevention/mitigation of, preparedness for, response to and recovery from emergencies affecting the Agency.

## 2. *Effective Date*

This policy takes effect on June 12, 2014.

It replaces the Emergency Management Policy dated 2008-02-08.

## 3. *Application*

This policy applies to all CBSA employees (permanent, term, casual and part-time), contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students.

All CBSA employees have an Emergency Management (EM) responsibility.

## 4. *Context*

EM is the management of emergencies concerning all hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery.

EM activities include:

- Identifying the risks that are within or related to the CBSA's area of responsibility, including those related to critical infrastructure;
- Preparing emergency management plans in respect to those risks;
- Developing, planning, maintaining, exercising and implementing those plans; and
- Providing training in relation to those plans.




## 5. Authorities

This policy is issued under the Emergency Management Act (2007, c.15), Subsection 6(1) and 6(2).

This policy is to be read in conjunction with its two appendices (Appendix A: The CBSA Strategic Emergency Management Plan; and Appendix B: The CBSA Event Management Framework).

## 6. Policy Statement

The CBSA is required to implement, monitor and maintain an emergency management program which will promote an integrated and resilient whole-of agency approach to emergency management planning.

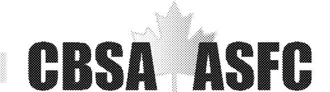
### 6.1 Policy Objective

The objective of this policy is to ensure that the Agency is equipped with a strategic, comprehensive and coordinated approach to emergency management activities. This involves the preparation, maintenance, testing, implementation, exercising and communications of emergency management plans, and training of personnel.

### 6.2 Expected Results

The expected results of this policy are:

- The Agency's EM risks are identified and evaluated regularly;
- EM plans are developed, maintained and updated in a timely fashion in respect to the identified EM risks;
- EM plans, processes and procedures are tested and exercised regularly; and
- Training is provided in relation to these EM plans.



# 7. Policy Requirements

**CBSA Employees (HQ and Regions)** are responsible for familiarizing themselves with their roles and responsibilities with their EM plans (if applicable), and immediately informing their manager/supervisor upon the discovery of an event/emergency affecting the Agency.

**CBSA Managers, Supervisors and Senior Management (HQ and Regions)** are responsible for familiarizing themselves with their roles and responsibilities within their EM plans (if applicable), ensuring that their staff are aware and fully trained on their individual roles, and notifying/informing the CBSA's 24/7 Border Operations Centre directly upon the discovery of an event/emergency affecting the Agency.

**Border Operations Centre (BOC)** is responsible for providing 24/7 support to the CBSA, as well as acting as the primary contact and conduit during events/emergencies affecting the Agency.

**Emergency Management (Comptrollership Branch)** is responsible for the establishment of this policy, overseeing compliance to this policy and its appendices, providing guidance and direction on this policy and ensuring the monitoring and oversight of this policy.

**Emergency Management (Operations Branch)** is responsible for creating, implementing, monitoring and exercising the operational elements of the Agency's Emergency Management policy, specifically with respect to the impact emergency situations have on daily operations and the delivery of the CBSA's mandate in the field.

## 7.1 Monitoring and Reporting Requirements

The Security and Professional Standards Directorate (SPSD) will periodically review the effectiveness of this policy. To support the review process, the SPSD plays an overarching role for the Agency's comprehensive EM program and is responsible for the monitoring

and tracking of EM activities. By doing such, the SPSD is able to ensure that the policy's objectives are pertinent and that all requirements are being adhered to.

Reporting to the President will occur bi-annually by means of the Agency's Strategic Emergency Management Plan (SEMP).

## *8. Consequences*

Consequences of non-compliance with this policy and its supporting guidelines may contribute to the CBSA not being able to prevent/mitigate, prepare for, respond to and recover from emergencies affecting the Agency. In essence, not following the Emergency Management Policy may render the Agency vulnerable.

## *9. Roles and Responsibilities*

### President / Executive Vice-President

- Ensures the effective implementation and governance of the Agency's comprehensive emergency management program;
- Provides direction for the overall emergency response and ensures that all levels of management within the CBSA integrate the emergency management requirements into their plans, programs, activities and services;
- Communicates and consults with internal and external stakeholders to strengthen the Agency's EM program; and
- Briefs the Minister of Public Safety Canada on the nature and extent of an emergency situation as required.

### Departmental Security Officer (DSO)

- Leads and coordinates the development of the Agency's comprehensive emergency management program;
- Acts as the primary contact during all security related emergencies/events;

- Develops and maintains a suite of policies, procedures, tools and communication and awareness products to support the implementation of the EM Policy throughout the Agency;
- Ensures strategies, plans and governance are in place to support the EM program;
- Ensures that managers and employees have access to the appropriate knowledge, understanding and tools required to fulfill their EM responsibilities;
- Develops and implements a Performance Measurement strategy for the Agency's comprehensive emergency management program;
- Communicates and consults with internal and external stakeholders to strengthen the Agency's EM program; and
- Provides briefings to Senior Management on the Agency's comprehensive EM program and its EM activities, as required.

## Vice-President, Operations Branch

- Leads the creation, implementation, monitoring and exercising of emergency-related plans and procedures for the Operations Branch, affecting all the Ports of Entry (POEs) and operational areas in the region;
- Acts as the primary contact during all operational related emergencies/events;
- Provides 24/7 support for the Agency and acts as the point of coordination for monitoring and reporting during events and/or emergency situations;
- Develops training, exercises and education of employees on procedures for responding to emergencies affecting the CBSA operations and mandate delivery;
- Coordinates a national approach to emergency management and operational readiness for all Ports of Entry; and
- Ensures communication and consultation with internal and external partners (international, national, provincial and local) to strengthen the Agency's ability to deliver its EM program.

## Vice-President, Information, Science and Technology Branch (ISTB)

- Acts as the primary contact during all IT related emergencies/events;

- Ensures disaster recovery plans are completed, tested and exercised;
- Develops IT security and continuity procedures for improved response and management of emergencies affecting CBSA operations;
- Provides input as Subject Matter Expert (SME) for international, federal/provincial and interdepartmental initiatives affecting IT Continuity;
- Ensures awareness of employees on procedures for responding to emergencies affecting CBSA IT continuity; and
- Ensures communication and consultation with internal and external partners (international, national, provincial and local) to strengthen the Agency's ability to deliver its EM program.

### Other Vice-Presidents

- Acts as the primary contact during emergency events affecting their respective branches;
- Ensures the timely completion of EM activities for their respective branches; and
- Ensures communication and consultation with internal and external stakeholders in order to strengthen the Agency's ability to deliver its EM program.

## *10. References*

- The Emergency Management Act (2007), Subsection 6.(1) and 6.(2).

### 11.1 Relevant Legislation, Regulations and Publications

- Public Safety Canada Federal Emergency Response Plan and related contingency plans;
- Public Safety Canada Federal Policy on Emergency Management;
- The *Customs Act*;
- *Canada Labour Code*, Part II;
- Canada Occupational Health and Safety Regulations, Part XVII;



- Treasury Board Secretariat Policy on Government Security; and,
- Communications Policy of the Government of Canada.

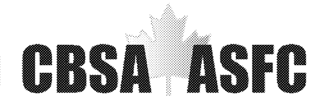
## 11. Enquiries

For more information, please contact:

Security and Professional Integrity Programs Division
Ottawa, Ontario K1A 0L8
Email: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

## 12. Appendices

- Appendix A – Strategic Emergency Management Plan
- Appendix B – CBSA Event Management Framework




# POLITIQUE SUR LA GESTION DES URGENCES

## *1. Préambule*

Conformément aux paragraphes 6(1) et 6(2) de la *Loi sur la gestion des urgences* (LGU), l'Agence des services frontaliers du Canada (ASFC) est chargée de la prévention/de l'atténuation, de la préparation, des interventions et du rétablissement associés aux urgences qui touchent l'Agence.

## *2. Date d'entrée en vigueur*

La présente politique entre en vigueur le 12 juin 2014.

Elle remplace la Politique sur la gestion des urgences qui date du 8 février 2008.

## *3. Application*

La présente politique s'applique à tous les employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels ou à temps partiel), au personnel embauché à contrat ou appartenant à une agence privée ainsi qu'aux personnes détachées ou nommées à l'Agence, étudiants compris.

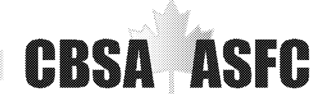
Tous les employés de l'ASFC ont une responsabilité en matière de gestion des urgences (GU).

## *4. Contexte*

La gestion des urgences s'étend à tous les risques, y compris toutes les activités et les mesures de gestion du risque liées à la prévention, à l'atténuation, à la préparation, à l'intervention et au rétablissement.

Les activités de GU comprennent les éléments suivants :

- déterminer les risques qui sont propres au secteur de responsabilité de l'ASFC ou qui y sont liés, notamment les risques concernant les infrastructures essentielles;
- préparer des plans de gestion des urgences à l'égard de ces risques;




- élaborer, planifier, tenir à jour, mettre à l'essai et mettre en œuvre ces plans;
- donner de la formation relativement à ces plans.

## 5. Autorisations

La présente politique est publiée en vertu de la *Loi sur la gestion des urgences* (2007, ch. 15), paragraphes 6(1) et 6(2).

La présente politique doit être lue en parallèle avec ses deux annexes (Annexe A : Plan stratégique de gestion des urgences de l'ASFC; et l'Annexe B : Cadre de gestion des événements de l'ASFC).

## 6. Énoncé de la politique

Il incombe à l'ASFC de mettre en œuvre, de surveiller et de tenir à jour un programme de gestion des urgences qui favorisera une approche globale, intégrée et solide de la planification de la gestion des urgences.

## 6.1 Objectif de la politique

L'objectif visé par la présente politique est de s'assurer que l'Agence est dotée d'une approche stratégique, globale et coordonnée en matière d'activités de gestion des urgences. Cela comprend la préparation, la tenue à jour, la mise à l'essai, la mise en œuvre, les communications des plans de gestion des urgences et la tenue d'exercices et d'activités de formation à leur sujet.

## 6.2 Résultats attendus

Les résultats attendus de la présente politique sont les suivants :

- les risques liés à la gestion des urgences à l'Agence sont cernés et évalués régulièrement;
- des plans de GU sont élaborés, tenus et mis à jour au moment opportun à l'égard des risques liés à la GU qui ont été cernés;

- les plans, processus et procédures de GU sont mis à l'essai et font régulièrement l'objet d'exercices;
- de la formation est offerte relativement à ces plans de GU.

## *7. Exigences de la politique*

**Les employés de l'ASFC (AC et régions)** doivent se familiariser avec leurs rôles et responsabilités relativement à leur plan de GU (s'il y a lieu) et informer immédiatement leurs gestionnaires ou superviseurs de la découverte d'un événement ou d'une situation d'urgence qui touche l'Agence.

**Les gestionnaires, les superviseurs et la haute direction de l'ASFC (AC et régions)** doivent se familiariser avec leurs rôles et responsabilités relativement à leurs plans de GU (s'il y a lieu), s'assurer que les membres de leur personnel connaissent leurs plans individuels et sont pleinement formés à cet égard, et avertir ou informer le Centre des opérations frontalières de l'ASFC ouvert en tout temps dès la découverte d'un événement ou d'une situation d'urgence qui touche l'Agence.

**Le Centre des opérations frontalières (COF)** doit fournir un soutien en permanence à l'ASFC et agir comme premier centre de ressources et d'exécution au cours d'événements ou de situations d'urgence touchant l'Agence.

**La Gestion des urgences (Direction générale du contrôle)** est responsable d'établir la présente politique, de surveiller l'observation de celle-ci de même que de ses annexes, de donner des directives et une orientation relativement à cette politique et d'assurer le contrôle et la surveillance générale de celle-ci.

**La Gestion des urgences (Direction générale des opérations)** est responsable de créer, de mettre en œuvre, de surveiller et d'exercer les éléments opérationnels de la Politique sur la gestion des urgences de l'Agence, particulièrement en ce qui a trait aux

répercussions des situations d'urgence sur les opérations quotidiennes et l'exécution du mandat de l'ASFC dans les bureaux locaux.

## *7.1 Exigence en matière de surveillance et de rapports*

La Direction de la sécurité et des normes professionnelles (DSNP) doit examiner périodiquement l'efficacité de la présente politique. Pour appuyer le processus d'examen, la DSNP joue un rôle de premier ordre à l'égard du programme global de GU de l'Agence et elle est chargée d'assurer la surveillance et le suivi des activités de GU. Ce faisant, la DSNP est en mesure de s'assurer que les objectifs de la politique sont pertinents et que l'on respecte toutes ses exigences.

Tous les deux ans, un rapport est présenté au président au moyen du Plan stratégique de gestion des urgences de l'Agence (PSGU).

## *8. Conséquences*

Le non-respect de la présente politique et de ses lignes directrices pourrait faire en sorte que l'ASFC n'est pas en mesure de prévenir ou d'atténuer les urgences qui pourraient la toucher  ou encore de s'y préparer, d'y réagir et d'assurer le rétablissement. En d'autres termes, le non-respect de la Politique sur la gestion des urgences peut rendre l'Agence vulnérable.

## *9. Rôles et responsabilités*

### Président / premier vice-président

- Voir à la mise en œuvre et à la gouvernance efficaces du programme global de gestion des urgences de l'Agence.
- Donner l'orientation pour l'ensemble des interventions d'urgence et veiller à ce que tous les paliers de gestion au sein de l'ASFC intègrent les exigences en matière de gestion des urgences dans leurs plans, programmes, activités et services.
- Communiquer avec des intervenants à l'interne et à l'externe et les consulter pour raffermir le programme de GU de l'Agence.

- Informer le ministre de Sécurité publique Canada sur la nature et la portée d'une situation d'urgence, suivant les besoins.

## Agent de sécurité du ministère (ASM)

- Diriger et coordonner l'élaboration du programme global de gestion des urgences de l'Agence.
- Agir comme principale personne-ressource au cours de situations d'urgence ou d'événements liés à la sécurité.
- Élaborer et tenir à jour une série de politiques, de procédures, d'outils et de produits de communication et de sensibilisation afin d'appuyer la mise en œuvre de la politique de GU dans l'ensemble de l'Agence.
- S'assurer que des stratégies, des plans et une structure de gouvernance sont en place pour appuyer le programme de GU.
- Veiller à ce que les gestionnaires et les employés aient accès aux connaissances et aux outils nécessaires pour assumer leurs responsabilités en matière de GU.
- Élaborer et mettre en œuvre une stratégie de mesure du rendement relativement au programme global de gestion des urgences de l'Agence.
- Communiquer avec des intervenants à l'interne et à l'externe et les consulter afin de raffermir le programme de GU de l'Agence.
- Donner des séances d'information à la haute direction au sujet du programme global de GU de l'Agence et de ses activités en la matière, selon les besoins.

## Vice-président, Direction générale des opérations

- Diriger la création, la mise en œuvre, la surveillance et l'exercice des plans et des procédures relatifs aux urgences pour la Direction générale des opérations, qui touchent les points d'entrée et les secteurs opérationnels de la région;
- Agir comme principale personne-ressource au cours de toutes les opérations liées à des événements ou à des situations d'urgence.

- Assurer un soutien en permanence au nom de l'Agence et agir comme point de coordination de la surveillance et de la présentation de rapports au cours d'événements ou de situations d'urgence.
- Mettre sur pied des formations, des exercices et des séances de sensibilisation concernant les procédures d'intervention face à des situations d'urgence touchant les opérations et l'exécution du mandat de l'ASFC.
- Coordonner une approche nationale de la gestion des urgences et de préparation opérationnelle pour tous les points d'entrée.
- Assurer des communications et des consultations avec des partenaires à l'interne et à l'externe (aux niveaux international, national, provincial et local) afin de renforcer l'Agence dans sa capacité à exécuter son programme de GU.

## Vice-président, Direction générale de l'information, des sciences et de la technologie (DGIST)

- Agir comme principale personne-ressource au cours de tous les événements ou situations d'urgence liés à la TI.
- Veiller à ce que des plans de reprise après sinistre soient mis au point, et fassent l'objet d'essais et d'exercices.
- Élaborer des procédures de sécurité et de continuité de la TI pour améliorer l'intervention et la gestion des urgences touchant les opérations de l'ASFC.
- Fournir un apport en tant qu'expert en la matière dans le cadre d'initiatives internationales, fédérales/provinciales et interministérielles touchant la continuité de la TI.
- Sensibiliser les employés aux procédures d'intervention face aux urgences touchant la continuité de la TI à l'ASFC.
- Assurer des communications et des consultations avec des partenaires à l'interne et à l'externe (aux niveaux international, national, provincial et local) afin de renforcer l'Agence dans sa capacité à exécuter son programme de GU.



## Autres vice-présidents

- Agir comme principales personnes-ressources au cours de situations d'urgence touchant leur direction générale.
- Voir à l'exécution en temps opportun des activités de GU pour leur direction générale.
- Assurer des communications et des consultations avec des intervenants à l'interne et à l'externe afin de renforcer l'Agence dans sa capacité à exécuter son programme de GU.

## *10. Références*

- *Loi sur la gestion des urgences* (2007), paragraphes 6(1) et 6(2).

### 11.1 Lois, règlements et publications pertinents

- Plan fédéral d'intervention d'urgence de Sécurité publique Canada et plans d'urgence connexes.
- Politique fédérale en matière de gestion des urgences de Sécurité publique Canada.
- *Loi sur les douanes.*
- *Code canadien du travail*, partie II.
- *Règlement canadien sur la santé et la sécurité au travail*, partie XVII.
- Politique sur la sécurité du gouvernement du Secrétariat du Conseil du Trésor Politique de communication du gouvernement du Canada.

## *11. Demande de renseignements*

Pour en savoir davantage, veuillez communiquer avec :

Division des programmes de sécurité et d'intégrité professionnelle
Ottawa (Ontario) K1A 0L8
Courriel: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca




## 12. Annexes

- Annexe A – Plan stratégique de gestion des urgences
- Annexe B – Cadre de gestion des événements de l'ASFC




# CBSA Event Management Framework

2013







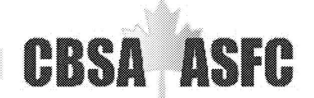




Canada Border Services Agency
Agence des services frontaliers du Canada



# Contents




## Purpose

The Canada Border Services Agency's (CBSAs) Event Management Process (EMP) outlines the model for a comprehensive management process across the entire Agency (Headquarters (HQ) and the Regions). It will be used to manage a wide range of events affecting the CBSA.

The EMP requires the identification of potential events, an assessment of their impact on the CBSA, and the implementation of an immediate and collaborative response.

The purpose of the EMP is to:

1. Identify a clear, concise and centralized event management process across the Agency;
2. Optimize efficiency of the CBSA operations through improved integration, planning, risk management, forecasting and reporting;
3. Improve intelligence and information sharing to support informed risk management decisions; and,
4. Facilitate decision making and event management by senior officials.

The EMP will strengthen the CBSA's capacity to notify its Emergency Management (EM) stakeholders as well as facilitate decision making and response to events affecting the Agency. Immediately engaging affected stakeholders during an event allows for a more collaborative and effective response to emergencies.

This document provides the guidelines and procedures for all employees within the Canada Border Services Agency to consistently implement the EMP.

This document does not however aim to provide direction or instructions for response to a specific incident or emergency event; rather it provides the framework for coordinating the event management activity of the Agency.

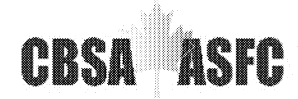
## Definitions

For the purpose of this process, and in keeping in touch with other areas of the Comprehensive Emergency Management Program, the following definitions should be used:

**Significant Event:** An event, either present or imminent, which has an impact on the Agency and its ability to maintain its critical services.

For example:

- A natural disaster (earthquake, flood…);
- An illegal migrant vessel ;
- Social unrest in another country (Syria, Egypt);
- Public Health event (pandemic, SARS);




- An event which results in the evacuation of a building, port of entry, (gas leak, suspicious package, fire…).
- A demonstration or protest at a CBSA facility attracting media attention; and
- Loss of an IT functionality at a CBSA facility impacting critical services (as defined below).

**Critical Service:** A service which, if unavailable, would result in a high degree of injury to the:

- Health/ safety/security/economic well-being of Canadians;
- Effective functioning of the Government of Canada; or
- CBSA's ability to deliver its mandate.

**Critical Security Incident:** An incident that has the potential to seriously affect the overall functions of the CBSA by causing serious injury or loss of life, significant property damage, threat to services/operations and/or partial or complete disruption of border operations. Critical Security Incidents must be reported immediately to the Regional Security Manager, followed by the BOC (if necessary).

For example:

- Abuse, threats, stalking and assaults against employees;
- Situations where clients threaten to commit suicide;
- Malicious codes and virus alerts/attacks against CBSA communication or computer systems or other circumstances leading to system degradation; or
- Demonstrations, occupations or unlawful entry into CBSA premises.

**Critical IT Security and Continuity Incident:** An incident that impacts the IT infrastructure and its ability to support the Agency's critical services. Critical IT Continuity and Security incidents must be reported immediately to the IT Response Centre (ITRC)

**Duty Executive (DE):** An identified executive responsible for providing oversight to the EMP by ensuring that events are thoroughly assessed, and that the response implemented by the Agency aligns with established processes and priorities. As such, the assigned Duty Executive will depend on the type of event. Duty executives have been identified for each Branch of the Agency.

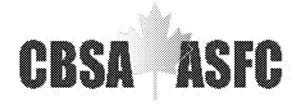


**Incident Command System (ICS):** The ICS is a model for command, control, and coordination of emergency response at an emergency site. It provides a safe way of coordinating the efforts of agencies and resources as they work together towards safely responding, controlling and mitigating an incident. The ICS improves event management through creating a common organizational structure and applying key management principles in a standardized way. Integration of the ICS in incident response ensures that the CBSA approach aligns with other government departments and Canadian law enforcement partners.

**Office of Primary Interest (OPI) / Subject Matter Expert (SME):** An office group and/or a person who provides expertise in a specific area or on a particular aspect of a response.

For example:
- Intelligence Assessment;
- Communications;
- Border Operations;
- Information Technology Security and Continuity; or
- Physical Security

**Surge Capacity:** The CBSA's Border Operations Centre (BOC) has been created with workspace to accommodate extra employees who can assist in the response to incidents. Subject Matter Experts (SMEs) from Other Government Departments (OGDs), CBSA Offices of Primary Interest (OPIs) and police forces may report to the BOC as liaisons should a situation of significant severity arise. Surge capacity creates flexibility to effectively respond to a wider range of incidents.




## Managing Events

A wide range of emergency management processes and theories must be applied to events and issues for effective management. The CBSA Event Management Process flow chart depicts the response to events which affect the Agency.

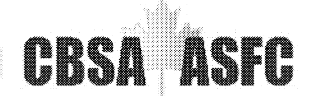
During a significant event, the BOC functions as the primary channel through which stakeholders, responders, and the OPI should communicate plans and outcomes. In this capacity, the BOC facilitates situational awareness through timely and effective communication between the OPI's, HQ, the Regions, Duty Executives and the President and/or Executive Committee (EC)

## Thresholds for Reporting

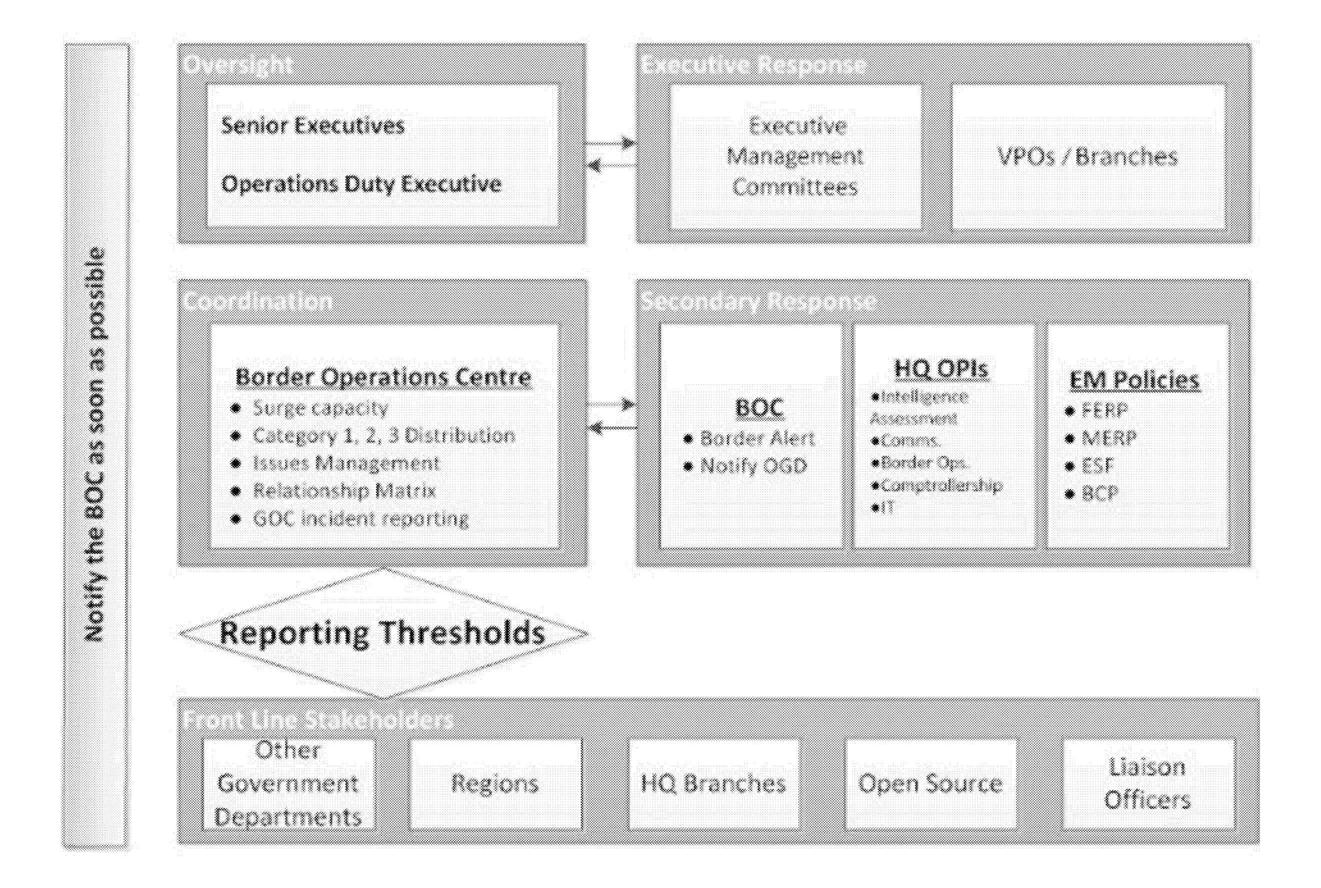
If you become aware of an event or a potential event, you should inform and consult with your manager/supervisor/ chain of command.  In extenuating circumstances where a manager/supervisor is not available or present, contact the BOC.

*Always remember, "When in doubt cc: the BOC"*

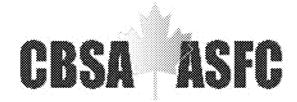
Examples of scenarios which require reporting can be found in Appendix B




**The CBSA Event Management Process – "Call the BOC"**




BCP – Business Continuity Plan
BOC – Border Operations Centre
EAP – Employee Assistance Program
EM – Emergency Management
ESF – Emergency Support Function
FERP – Federal Emergency Response Plan
GOC – Government Operations Centre
MERP – Marine Event Response Protocol
OPI – Office of Primary Interest
RDG – Regional Director General
ROC – Regional Operations Centre
VPO – Vice-President's Office



# The CBSA Event Management Process

## *Prevention/Mitigation of an Event*

As planning and preparedness methods and in order to mitigate the effects of an event should one occur, the CBSA has established the following preventative techniques:

**CBSA Today:** Daily, a report aimed to promote awareness to management through forecasting, monitoring, and reporting on situations that impact the Agency is prepared by the BOC. Regions and select OPI's are expected to feed into this report by providing details about activities and events that affect their operations.

**Issues Management:** Every business day, an Issues Management conference call is scheduled at 08:15 EST. During these conference calls representatives from multiple CBSA branches collaboratively identify and manage hot issues affecting the Agency. This process provides a coordinated response through the use of a standard issues management process, documents, and tools.

**Executive Branch Management Roster (EBMR):** the EBMR is a weekly listing of designated contacts for each branch that will be available to respond should the Duty Executive or senior executives require information regarding one of their business lines. It is updated by the BOC weekly.

**Intelligence Cycle:** The Intelligence Cycle is used to transform the unknown and the uncertain into the known through the effective and skilful use of the intelligence method. Transforming information into intelligence enables the CBSA to work towards effectively and confidently preventing/mitigating events. The Enforcement and Intelligence Operations Directorate uses the intelligence cycle to develop intelligence cases and the BOC has adapted this intelligence cycle to prevent/mitigate and/or reduce risks related to emergencies.

**Emergency Management Plans (EMPs):** Based on the identification of potential priority risks affecting the Agency, pre-established procedures are developed in order to ensure the earliest possible response to a specific emergency. When established processes exist, they must be followed throughout the emergency management process to the reasonable extent given the unique circumstances presented by the situation.

**Business Impact Analysis (BIA):** Based upon the Agency's analysis of identifying critical business functions and workflows, determining the qualitative and quantitative impacts of a disruption, and prioritizing recovery objectives and establishing time frames.

**Business Continuity Plans (BCPs):** Agency plans containing documented procedures that guide the Agency to respond, recover, resume and restore to a pre-defined level of operation following the critical service incident.

**Disaster Recovery Plans (DRP):** Clearly defined and documented plans which recover IT capabilities when a disruption occurs.




## Upon the discovery of an event

Upon the discovery of an event, the following procedures are to be followed:

1) The manager/supervisor should be notified immediately. Other than emergency services, the manager/supervisor should always be the first point of contact once an event is identified, they will then inform the BOC.
2) Once the BOC receives information concerning an event they will gather as many details surrounding the event as possible. As a minimum, BOC officers will likely seek the following information from the provider:
    a. Name and contact details of the information provider
    b. Incident description, date/time of occurrence
    c. Scope-local/regional/national
    d. Current status (new/update/resolved/unresolved/unchanged)
    e. Is the information protected by third party rule
    f. Lead department and/or other players
    g. Impacts (economy, national security, flow of traffic, media)
    h. Individuals notified (ex: Has the DSO or RDG been advised?)
3) The BOC in consultation with OPI's and the Duty Executive will provide the initial assessment of the event and conclude whether the event is significant. If the event is determined to be "not significant" the EMP stops here and the BOC continues to monitor the event.
4) If deemed significant, the BOC will work with the appropriate Duty Executive to confirm:
    a. If reporting is required, and if so, the level and scale of reporting required
    b. If members on the CBSA Executive Branch Management Roster (EBMR) should be advised
    c. If the Minister's office should be advised
    d. If the Government Operations Centre should be advised
    e. If any additional action is required.

## Managing the Event

1) The Offices of Primary Interest (OPI) along with Subject Matter Experts (SME) will respond to the event and work using the Incident Command System. The nature of the event will determine the OPI.
2) The BOC will establish a reporting threshold and set timelines for reporting from:
    a. HQ Branches
    b. Regions
    c. Other Government Departments
    d. Liaison Officers
    e. Open Sources
3) HQ Branches, the Regions, OGD, Liaison Officers and Open Sources will provide the BOC with timely situational reports as per the established reporting timelines.
4) The BOC will then use the following methods/techniques to aid in the management of the significant event:
    a. Intelligence cycle

   b. Issues Management
   c. Relationship matrix
   d. Surge Capacity
5) The BOC will report to the Duty Executive who will provide executive oversight of the event management process.
6) The Duty Executive will determine if members of the CBSA Executive Committee (EC) should be consulted for subject matter expertise.
7) For extreme significant events the Duty Executive will report up to the President of the CBSA who will provide direction for the overall emergency response.

### *Upon the conclusion of the event*

At the conclusion of the event:

1) The BOC will prepare and share a "Significant Event Conclusion" message with the established distribution list. This message ensures that everyone is aware that the significant event has concluded.
2) The OPI will coordinate a Hot Wash meeting to discuss the lessons learned from the significant event and, if necessary, prepare an After Event Report.
3) The Duty Executive will review and approve the After Event Report.

## Responsibilities during an Event

Comprehensive emergency management across the Agency is a discipline that requires the integration of various stakeholders working as a cohesive unit to ensure the successful planning and preparedness for mitigation of and recovery from significant events. The following groups have key responsibilities in the CBSA's Event Management Process:

**CBSA Managers/Supervisors/Chiefs (HQ and Regions)**

- Upon the discovery of an event, CBSA managers should contact and notify the CBSA's 24/7 Border Operations Centre at:
    - Telephone:
    - MITNET:
    - Blackberry PIN:
    - E-mail: boc-cof@cbsa-asfc.gc.ca
- **** Other than emergency services, the BOC should always be the first point of contact upon the identification of an event.*

**All CBSA Employees**

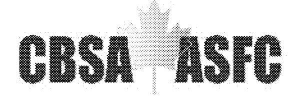
- Upon discovery of an event, CBSA employees should immediately advise their managers/supervisors.
- In cases of extenuating circumstances in which a manager is not present, employees should contact the CBSA's 24/7 Border Operations Centre directly.

  **** Other than emergency services, the manager/supervisor should always be the first point of contact upon the identification of an event.*

**Duty Executive (DE)**

The responsibilities of the Duty Executive include but are not limited to:

- Leading the response efforts as the OPI and provide executive oversight to the BOC for the Event Management Process;
- Determining the appropriate type of distribution of information regarding events as well as the reporting tempo. Options for distribution are identified in **Appendix A – Methods of distribution;**
- Determining if members of the CBSA Executive Committee (EC) should be consulted for subject matter expertise;
- Prioritizing the response efforts and making the final decision regarding actions taken within the EMP;
- When necessary, briefing the President on impacts and actions taken to deal with significant events; and,
- Approving media outputs (in conjunction with the Communications Directorate).



**Issues Management Process**

The Issues Management process is designed to quickly identify and respond to issues affecting the CBSA. The purpose of the Issues Management Process is to ensure that the appropriate people have the correct information at the right time to ensure the most effective action can be taken. This includes but is not limited to:

- Notifying affected internal stakeholders;
- Preparing case summaries, senior management briefings, and program impact assessments;
- Identifying OPI;
- Seeking additional information when appropriate;
- Stopping aggravating factors from escalating inappropriately or unduly;
- Identifying and planning for potential new developments; and,
- Monitoring issue developments and providing situational awareness to affected stakeholders.

**The Border Operations Centre**

The responsibilities of the Border Operations Centre include but are not limited to:

- Providing 24/7 support to the CBSA;
- Acting as a primary contact during a significant event when there is an identified impact to the Agency's operational mandate delivery;
- Once an event is identified as being significant by the Duty Executive, acting as the primary conduit and central hub through which stakeholders (HQ branches, Regions, Other Government Departments, Liaison Officers, Open Sources, etc.) will coordinate events;
- Initiating surge capacity within the BOC, when necessary;
- Coordinating the response to events by activating particular SOP, by arranging conference calls, engaging the Executive Branch Management Roster, implementing existing protocols, and establishing working groups;
- Providing a centralized significant event notification service within the Agency;
- Promoting awareness of events by providing notifications to the CBSA and OGDs; and
- Communicating a message to the event notification distribution list stating the event has concluded.

**Emergency Management, Operations**

The responsibility of the Emergency Management Section, Operations Branch includes but is not limited to:

- Assessing and providing subject matter expertise and guidance regarding the impacts of an emergency situation which affects the Agency's ability to continue delivery of its operational mandate;

- Offering support to the BOC should they require assistance with resource or subject matter expertise with respect to the elements included in existing preparedness, mitigation, or whole-of-government plans;
- Acting as the liaison officer (as required) to the Government Operations Centre (GOC) to ensure CBSA integration into a potential larger/whole of government response to an emergency; and
- Leading or assisting in the facilitation of a Hot Wash and after action reporting process of an operational incident not otherwise pertaining to IT, infrastructure and Security incidents.

**Emergency and Business Continuity Management, Comptrollership**

The responsibilities of the Emergency and Business Continuity Management Section, Comptrollership Branch, include but are not limited to:

- Acting as the central agency repository and ensuring accuracy of all Business Continuity Plans and related data for the Agency; and
- Leading in the coordination of After Action Reporting and Improvement Action Planning for events affecting the Agency (more than one Branch).

**Critical Services Managers**

The responsibilities of Critical Services Managers include but are not limited to:

- Activating their plans(s) when required, advising the BOC accordingly and providing timely status updates;
- Coordinating the essential operating staff and facilitating in order to sustain operational capability for an extended period as described in the BCP;
- Deactivating their plan(s) when business returns to normal and completing the follow up reports.

**Information Technology Response Centre (ITRC)**

The responsibilities of the Information Technology Response Centre include but are not limited to:

- Acting as primary IT contact during a significant event and providing after hours support (the ITRC is the central and only contact within ISTB in a disaster);
- Liaising with the Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC);
- Ensuring CBSA responds according to the Government of Canada IT Incident Management Plan (GC IT IMP);
- Liaising with the Canada Revenue Agency (CRA);
- Communicating and coordinating ISTB response with CBSA stakeholders and the BOC;
- Coordinating and ensuring BCP or Disaster Response Plans are implemented as required;

- Analyzing non-technical significant events for possible technical impacts or response strategies;
- Providing regular situational updates to the BOC, when requested;
- Providing liaison officers to the Canadian Incident Cyber Response Centre (CICRC) should the incident involve other government departments or become a national issue;
- Acting as the liaison officer (as required) to the Government Operations Centre (GOC) to ensure CBSA integration into a potential larger/whole of government response to an emergency; and
- Leading the Hot Wash following an IT focused significant event.

**Security and Professional Standards**

The responsibilities of Security and Professional Standard, Comptrollership Branch, include but are not limited to:

- Acting as the primary contact during security related events and providing after hours support;
- Managing and updating the Agency Employee Notice Line (ENL) for the National Capital Region (NCR);
- Coordinating the response of Building Emergency Organization Teams within the CBSA facilities;
- Assisting in the evacuation of buildings;
- Coordinating movement of key personnel to alternate locations;
- Providing access to the CBSA floor space (controlling the ID/Access Card Program);
- Providing regular situational updates to the BOC, when required;
- Leading the Hot Wash following a security focused emergency event; and
- Developing After Action and After Event reports for issues affecting security.

**Infrastructure and Environmental Operations**

The responsibilities of Infrastructure and Environmental Operations, Comptrollership Branch, include but are not limited to:

- Reporting the incident to the PWGSC National Service Call Centre;
- Liaising with building landlords and PWGSC property management;
- Maintaining and providing HQ buildings distribution lists to the BOC for emergency updates to employees;
- Developing, translating and dispatching building notices and updates to CBSA employees in the buildings affected by an event by e-mail;
- Providing regular situational updates to the BOC, when requested; and
- Leading the Hot Wash following an accommodation focused significant event.




**Communications**

The responsibilities of Communications, Corporate Affairs Branch, include but are not limited to:

- Providing communications planning, analyses and advice to the "incident" OPI and Agency senior management, and training CBSA spokespersons as required;
- Managing Agency public communications produced by the Agency, including responding to media inquiries, maintaining the Internet site and the main pages of Atlas, and posting information via Social Media channels;
- Liaising with Public Safety Communications and the Minister's Office, as well as other Government of Canada departments/agencies as required;
- Providing Emergency Communications support to the BOC, when required;
- Organizing media events to communicate significant event-related information to the public;
- Providing communications support to employees and their families directly impacted by the event/crisis; and,
- Supporting other areas in developing products for communicating to employees, including training CBSA spokespersons as required, editing and revising messages and other products, deploying distribution channels, as required.

**Human Resources**

The responsibilities of the Human Resource Branch include but are not limited to:

- Acting as the primary contact during HR-related significant events;
- Providing advice and guidance to management regarding leave and collective agreement entitlements;
- Providing information to affected employees about the services of the Employee Assistance Program;
- Providing advice and guidance to management on the legislative requirements for ensuring the safety of employees; and
- Leading the Hot Wash following an HR related significant event.

**Regional Emergency Management Coordinator**

The responsibilities of the Regional Emergency Management Coordinators include but are not limited to:

- Providing the link between the HQ Emergency Management Section and the Regional Management Team;
- Providing support to regional operations and headquarters on emergency management related issues;
- Ensuring that a collaborative relationship exists within the region including Regional Security Officers, Regional Occupational Health and Safety Advisors and Regional Labour Relations Advisors;
- Ensuring Regional Emergency Operation Centre facilities and alternate site locations are available for use during an emergency (including supplies and equipment) and that communication has been established with the Border Operations Centre during events;

- Preparing and maintaining emergency related reporting mechanisms between headquarters and regional management; and
- Providing regular situational updates to the BOC, when required.

**Senior Building Officer/Responsible Building Authority (RBA)**

The responsibilities of the Senior Building Officer / Responsible Building Authority (RBA) include but are not limited to:

- Preparing and administering the fire safety plan;
- Ensuring that physical fire protection features in the building are maintained;
- Ensuring that an Emergency Organization exists and that it follows the requirements of the fire safety plan;
- Holding fire drills and meetings;
- Assisting the Chief Building Emergency Officer with the building fire safety plan;
- Appointing an alternate RBA;
- Instructing the Chief Building Emergency Officer to initiate search or evacuation procedures in relation to bomb threats and other emergencies (with the exception of fire); and,
- Ensuring that the Director, Fire Protection Services and Labour Programs of Human Resources Development Canada, in advised of all fires and other building evacuations in accordance with Treasury Board standards.

**Chief Building Emergency Officer**

The responsibilities of the Chief Emergency officer include but are not limited to:

- Overseeing the day-to-day fire protection/prevention requirements in accordance with the applicable Codes for fire safety planning and emergency organizations;
- Preparing, implementing and administering an approved Building Evacuation Plan as part of an emergency procedure plan for his/her building;
- Establishing, maintaining and administering the Fire and Emergency Organization;
- Assuming full authority for control of the Fire and Emergency Organization and with the assistance of the building superintendent for the evacuation of the building occupants until such time as the emergency terminates of the Fire Department arrives at the scene and assumes responsibility;
- Remaining in control of the evacuation process and liaising with the Municipal Fire Department; and,
- Appointing a Deputy Chief Building Emergency Officer.




## Appendix A – Methods of Distribution

There are various methods of distribution available through the BOC.

### 1. *CBSA Calendar*

The CBSA Calendar is maintained by the National Border Operations Centre (NBOC) in Microsoft Outlook. It contains information regarding future events. The purpose of the CBSA Calendar is to create a no surprise environment for CBSA executives and CBSA Operations Branch. Clients with access to the CBSA Calendar include executives within HQ and the regions, executive assistants, key content providers and representatives from key HQ OPIs.

### 2. *CBSA Today*

The Border Operations Center (BOC) began publishing the *CBSA Today* for senior executives in October 2010. Since its creation, the report's scope and audience has gradually but significantly increased. The Vice-President of Operations is now encouraging the use of the *CBSA Today* during shift-briefings for Border Services Officers across Canada. The *CBSA Today* is distributed each business day at 08:30 EST.

### 3. *Advisory*

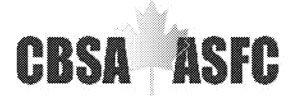
All events which the BOC becomes aware of are considered for a Significant Event Notification (SEN). The BOC provides an advisory only to the affected stakeholders for events which do not meet the SEN threshold. There are established key groups of affected stakeholders which the BOC may select for notification including: Communications; International Operations; Legal; Targeting Operations; Intelligence; Human Resources; Regions; Operational Reporting, or any other CBSA OPI.

### 4. *Border Wait Time (BWT) Notification*

A BWT notification must be provided for all BWT that are 60 minutes or greater as a result of normal heavy traffic. A BWT that is directly related to a significant event such as a bomb threat or flooding at a POE will be reported with a Category 1, 2, or 3 SEN. The BOC has additional procedures on file for implementing this outcome.

### 5. *Limited Distribution*

For information that is both sensitive and urgent, the BOC will identify a targeted audience specific to the issue. Although the number of recipients is greatly reduced for limited distributions, the content format is similar to an advisory or a notification.



## 6. *Situation Reports*

For large scale events such as the G8/G20 the BOC consolidates information from multiple CBSA and other government department stakeholders to create a single report at scheduled intervals. Separate situation reports are normally created for internal CBSA distribution and distribution to OGDs.

The threshold for implementing situation reports generally requires events to be of a significant enough nature to be of interest to the Privy Council Office, or the Office of the Prime Minister. Typically they would require the consolidation of information from multiple CBSA regions, or from multiple OGDs. Situation reports may however also be implemented in response to an event when updates will be required over a lengthy period of time. Special instruction regarding the reporting tempo and content should be provided to affected stakeholders. Special attention must be given to the internal and external distribution of information, and to the scheduled intervals of inbound and outbound reporting. The BOC Manager and Advisors are available to assist in these decisions based on responses to past events.



## Appendix B – Thresholds for Reporting

**Operations:**

- Border wait times greater than one hour;
- Events that may cause border closures/delays in either direction;
- Events causing significant impact to transportation modes;
- Natural disasters: earthquakes, floods, significant storms;
- Use of Force incidents or deployment of oleoresin capsicum spray/baton/firearm;
- Incident involving firearm(s) discharge *(intended or not);*
- Significant staff relations issues/ labor action concerns;
- Facility evacuations; and,
- Flight diversions or emergency landings.

**Media Implications:**

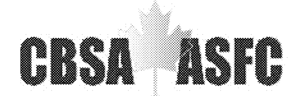
- Events involving a prominent individual/delegate that may attract media interest (A prominent individual with complications on clearing CBSA, with admissibility concerns, an enforcement action, a seizure, removal, detention, allowed to leave);
- Incidents or Access to information Requests that may result in serious complaint/media interest;
- CBSA activity or event that is causing or may cause media attention; and,
- Press releases or media coverage that refers to or has an impact upon CBSA activities.

**IT Issues:**

- Technical problems/unscheduled system outages; and,

**Public Safety/Health Issues:**

- Threats/incidents related to public health;
- Threats/incidents related to food supply chain or agriculture;
- Threats/incidents related to Canada's safety and security;
- Threats/incidents that may have national security context;
- Threats/incidents involving chemical, biological, radiological, nuclear or explosives (CBRNE); and,
- Security incidents affecting international flights within or on route to Canada.



**Security:**

- CBSA employee harmed, injured or assaulted;
- Threat to CBSA employee;
- Damage or threats to physical CBSA assets or infrastructure (i.e. fire, theft, power outage, significant damage to premises);
- Member of the public is seriously injured at port of entry; and,
- Any incident involving death.



# Building Emergency Response Planning

## 1. Purpose

The purpose of this policy is to provide the Canada Border Services Agency (CBSA) with a structured approach to ensure the safety of employees and visitors in its facilities during any emergency situation.

## 2. Effective Date

This policy takes effect on 2015-01-30.

It replaces the policy on Building Emergency Planning dated 2008-02-08.

## 3. Application

This policy is applicable to all visitors, employees (permanent, term, casual, and part-time), contract and private agency personnel and to individuals seconded or assigned to CBSA, including students.

This policy also applies to any other individuals required to comply with the health and safety requirements from the Canada Labour Code, Part II, and the Canada Occupational Health and Safety Regulations, Part XVII by virtue of a contract or a Memorandum of Understanding (MOU) with the CBSA.

## 4. Context

Many parties share the responsibility for ensuring the health and safety of federal employees working in a federally administered office building. Operating and maintaining the buildings, their systems and equipment, and planning for emergencies within the buildings are two critical activities intended to reduce the risks to the health and safety of federal employees.

The goal of building emergency planning is to save lives, prevent injuries, and protect property and information if an emergency occurs. Natural hazards, accidents and man-made emergency situations often occur unexpectedly and people are injured, information destroyed, and equipment and property damaged.

This policy commits the CBSA to maintain the principle of a high level of safety in all of its facilities through a well-organized and immediate response to any emergency situation.







## 5. Authorities

This policy is in accordance with the Canada Labour Code Part II, Part XVII, the Canada Occupational Safety and Health Regulations, the Policy on Government Security (PGS), and the requirements of the National Fire Code of Canada regarding emergency planning.

This policy is to be read in conjunction with:

- The Policy on Government Security (PGS)
- The Canada Labour Code, Part II: Occupational Health and Safety
- The Canada Occupational Safety and Health Regulations:
  - Part XVI, First Aid
  - Part XVII, Safe Occupancy of the Work Place
- The Treasury Board Standards – Standard for Fire Safety Planning and Fire Emergency Organization - Chapter 3-1
- The Emergency Management Act

## 6. Policy Statement

In each facility occupied by Canada Border Services Agency (CBSA), a Building Emergency Response Plan (BERP) based on a risk analysis must be developed, maintained, tested and communicated to prepare for and respond to any emergency situation that may occur (i.e. fire, bomb threat, armed robbery, explosion, earthquake, etc.) at that location.

## 6.1 Policy Objective

The objective of this policy is to ensure the safety and welfare of the Agency's employees and visitors and the protection of Agency assets while promptly responding to an emergency.

## 6.2 Expected Results

In each facility occupied by the CBSA, there is an emergency response plan aligned with the requirements of the Occupational Health and Safety Regulations Part XVII, and the Treasury Board's Standard for fire safety planning and fire emergency organization that includes:

- An Emergency Evacuation Plan that comprises procedures for the safe evacuation of a building and/or facility; and,
- Based on a risk analysis, procedures for all possible emergency situations at a building and/or facility, such as fires, bomb threats, armed robberies, hostage takings, earthquakes, chemical or environmental accidents, etc.







## 7. Policy Requirements

The Agency must ensure that, in each facility occupied by the CBSA:

- An Agency building official or a Responsible Building Authority (RBA) is identified;
- Building Emergency Organizations (BEO) are established in buildings for which they are required as per the occupancy requirements;
- A risk analysis is conducted to provide awareness and understanding of the environment. This includes an analysis of both internal and external factors, such as building location, as well as assets and emergency services which could impact or influence how an organization responds to and manages an emergency;
- Emergency response plans must be tested regularly;
- All incidents/events/issues that relate to the Incident Reporting Criteria must be reported to regional management and to the Border Operations Center (BOC) by phone at 613-960-6001 or by email to: boc-cof@cbsa-asfc.gc.ca.
- All incidents must be reported to Regional Security Officers and in Headquarters to HQ Security Officers, and to the Security and Professional Standards Directorate (SPSD).

.

### 7.1 Monitoring and Reporting Requirements

The Security and Professional Standards Directorate is responsible for the establishment of this policy, overseeing compliance to this policy and its appendices, providing guidance and direction on this policy and ensuring the monitoring and oversight of this policy.

Regional Security and in Headquarters HQ Security, will monitor the compliance of this policy within their Regions.

The Internal Audit and Program Evaluation Directorate may provide an independent level of assurance by performing internal audits. The results of these audits are reported to the Treasury Board Secretariat.

## 8. Consequences

Consequences of non-compliance with this policy and its supporting guidelines may contribute to the CBSA not being able to provide for the safety and welfare of its employees and visitors during an emergency. In essence, not following a Building Emergency Response Plan, when necessary, may render the Agency vulnerable.







The Departmental Security Officer (DSO) is responsible for addressing issues that arise regarding compliance with this policy and ensuring that appropriate remedial actions are taken to address these issues. Measures can include investigations, reports to Senior Management Committees, formal direction on corrective measures and close monitoring.

## 9. Roles and Responsibilities

All CBSA Employees are responsible for being familiar with the Building Emergency Response Plan procedures for their building, and being aware of their roles and responsibilities within the plan.

Consult Appendix A for a detailed description of the roles and responsibilities.

## 10. Enquiries

For more information, please contact:
Security and Professional Integrity Programs Division
410 Laurier Avenue West
Ottawa, Ontario, K1A 0L8
Email: Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca







# Planification d'urgence pour les immeubles

## 1. Objet

Le but de la présente politique est de fournir à l'Agence des services frontaliers du Canada (ASFC) une approche structurée pour assurer la sécurité des employés et des visiteurs dans ses installations au cours de toute situation d'urgence.

## 2. Date d'entrée en vigueur

La présente politique entre en vigueur le 30 janvier 2015.

Elle remplace la politique sur la planification d'urgence pour les immeubles du 8 février 2008.

## 3. Champ d'application

La présente politique s'applique à tous les visiteurs et à tous les employés de l'ASFC (permanents, temporaires, occasionnels et à temps partiel), aux employés contractuels et au personnel des organismes privés ainsi qu'aux personnes détachées ou affectées à l'ASFC, y compris les étudiants.

La présente politique s'applique également à toute autre personne qui est tenue de se conformer aux exigences en matière de santé et de sécurité de la Partie II du Code canadien du travail et de la partie XVII du Règlement canadien sur la santé et la sécurité au travail en vertu d'un marché ou d'un protocole d'entente (PE) conclu avec l'ASFC.

## 4. Contexte

De nombreuses parties partagent la responsabilité d'assurer la santé et la sécurité des fonctionnaires fédéraux travaillant dans un immeuble administré par le gouvernement fédéral. L'exploitation et l'entretien des immeubles, de leurs systèmes et de leurs équipements et la planification d'urgence pour ces immeubles sont deux activités essentielles destinées à réduire les risques pour la santé et la sécurité des employés fédéraux.

L'objectif de la planification d'urgence pour les immeubles est de sauver des vies, de prévenir les blessures et de protéger les biens et les informations dans l'éventualité d'une urgence. Les dangers d'origine naturelle, les accidents et les situations d'urgence d'origine humaine surviennent souvent de façon inattendue. Des personnes sont alors blessées, des informations sont détruites et des pièces d'équipement et des biens sont endommagés.







La présente politique engage l'ASFC à respecter le principe selon lequel un niveau élevé de sécurité doit être maintenu dans l'ensemble de ses installations par une intervention bien organisée et immédiate en cas de situation d'urgence.

## 5. Instruments habilitants

La présente politique est conforme à la Partie II du *Code canadien du travail*, à la partie XVII du *Règlement canadien sur la santé et la sécurité au travail*, à la *Politique sur la sécurité du gouvernement (PSG)* et aux exigences du *Code national de prévention des incendies du Canada* en matière de planification d'urgence.

Elle doit être lue en parallèle avec les documents suivants :

- Politique sur la sécurité du gouvernement (PSG);
- Code canadien du travail, Partie II, Santé et sécurité au travail;
- Règlement canadien sur la santé et la sécurité au travail;
  - Partie XVI, Premiers soins;
  - Partie XVII, Séjourner en sécurité dans un lieu de travail;
- Norme du Conseil du Trésor pour le plan d'évacuation d'urgence et l'organisation des secours en cas d'incendie – Chapitre 3-1;
- Loi sur la gestion des urgences.

## 6. Énoncé de politique

Dans chaque immeuble occupé par l'Agence des services frontaliers du Canada (ASFC), il faut établir, tenir à jour, mettre à l'essai et communiquer un plan qui permet de réagir à toute situation d'urgence qui pourrait se produire (incendie, alerte à la bombe, vol à main armée, explosion, séisme, etc.) à cet endroit à la lumière de l'analyse des risques recensés.

## 6.1 Objectif de la Politique

L'objectif de la présente politique est d'assurer la sécurité et le bien-être des visiteurs et des employés de l'Agence ainsi que la protection des biens de l'Agence, tout en permettant une intervention rapide en cas de situations d'urgence.

## 6.2 Résultats escomptés







Dans chaque installation occupée par l'ASFC se trouve un plan d'intervention en cas d'urgence conforme aux exigences de la Partie XVII du Règlement canadien sur la santé et la sécurité au travail et à la Norme du Conseil du Trésor pour le plan d'évacuation d'urgence et l'organisation des secours en cas d'incendie, qui comprend ce qui suit :

- un plan d'évacuation d'urgence qui inclut des procédures pour l'évacuation sécuritaire d'un immeuble ou d'une installation;
- des procédures, fondées sur une analyse des risques, pour toute situation d'urgence qui pourrait se produire dans un immeuble ou une installation (incendie, alerte à la bombe, vol à main armée, prise d'otages, séisme, incidents chimiques ou environnementaux, etc.).

## 7.0 Exigences de la politique

L'Agence doit s'assurer que, dans chaque installation occupée par l'ASFC :

- un agent responsable du bâtiment pour l'Agence ou une autorité responsable de l'immeuble (ARI) est désigné;
- des organismes de secours de l'immeuble (OSI) sont établis lorsque leur présence est requise dans certains bâtiments conformément aux exigences relatives à l'occupation;
- une analyse des risques est effectuée pour assurer une meilleure connaissance et une meilleure compréhension de l'environnement – cette analyse porte notamment sur des facteurs tant internes qu'externes, comme l'emplacement de l'immeuble ainsi que les biens et les services d'urgence qui pourraient avoir une incidence sur la façon dont un organisme intervient en situation d'urgence ainsi que sur sa gestion de cette situation;
- les plans d'intervention d'urgence sont mis à l'essai de façon régulière;
- tous les incidents, événements, ou problèmes, liés aux Critères de signalement des évènements sont signalés à la gestion régionale et au Centre national des opérations frontalières par téléphone au 613-960-6001 ou par courriel à : boc-cof@cbsa-asfc.gc.ca.
- toutes les incidents sont déclarées aux agents régionaux de la sécurité et pour l'Administration centrale, aux agents de la sécurité de l'AC, et à la Direction de la sécurité et des normes professionnelles (DSNP).

## 7.1 Exigences en matière de surveillance et d'établissement de rapports







La Direction de la sécurité et des normes professionnelles est tenue de mettre en œuvre la présente politique; de voir au respect de la politique et de ses annexes; de fournir des conseils et une orientation ainsi que d'effectuer des activités de suivi et de contrôle à l'égard de la présente politique.

Les agents régionaux de la sécurité et les agents de la sécurité pour l'Administration centrale veilleront au respect de la présente politique dans leur région.

La Direction de la vérification interne et de l'évaluation des programmes offrira un niveau d'assurance indépendant en effectuant des vérifications internes. Il faut rendre compte des résultats de ces vérifications au Secrétariat du Conseil du Trésor.

## 8. Conséquences

Les conséquences du non-respect de la présente politique et des directives à l'appui peuvent contribuer à empêcher l'ASFC de voir à la sécurité et au bien-être de ses employés et de ses visiteurs en situation d'urgence. En fait, le non-respect du plan d'intervention en cas d'urgence de l'immeuble peut, le cas échéant, placer l'Agence dans une situation de vulnérabilité.

L'agent de sécurité ministériel (ASM) est responsable de l'examen des questions qui se posent à l'égard de la présente politique et de veiller à ce que des mesures correctives appropriées soient prises à l'égard de ces problèmes. Ces mesures peuvent inclure des enquêtes, des rapports à l'intention des comités de la haute direction, des directives officielles sur les mesures correctives à prendre ainsi qu'une surveillance étroite.

## 9. Rôles et responsabilités

Tous les employés de l'ASFC sont tenus de se familiariser avec les procédures du plan d'intervention en cas d'urgence de leur immeuble et de connaître la nature de leurs rôles et de leurs responsabilités prévus dans ce plan.

Consulter l'annexe A pour obtenir une description détaillée des rôles et des responsabilités.

## 10. Demandes de renseignements

Pour de plus amples renseignements, communiquer avec :
Division des programmes de sécurité et d'intégrité professionnelle
410, avenue Laurier Ouest
Ottawa (Ontario) K1A 0L8
Courriel : Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca







# Appendix A: Building Emergency Response Directive

## 1. Introduction

This document provides procedures and guidelines necessary for the development of effective emergency plans and organizations. A detailed model of a Building Emergency Response Plan is outlined in Appendix A. It illustrates the information and essential elements that should be included in emergency plans. For threat specific information, please refer to the appropriate appendices in this Chapter.

A coordinated approach must be undertaken with stakeholders for the development and review of all Building Emergency Response Plans (BERP). Such stakeholders could include but are not limited to:

- Occupational Health and Safety Committee;
- Other tenants of the building & other government departments;
- Property managers;
- Property managers of neighbouring buildings;
- Municipal emergency coordinators as applicable (Police, Fire Prevention Services, Hazmat teams, etc.);
- Municipal public health units;
- Bridge Authority, Airport Authority;
- Brokers;
- US Customs.

## 2. Responsibility for the Development and Administration of the Building Emergency Response Plan

In all buildings occupied solely by the Canada Border Service Agency (CBSA), or in buildings where the CBSA has the largest number of employees, the most senior CBSA official is considered to be the Responsible Building Authority (RBA) and must ensure that emergency plans are developed and maintained.

In buildings occupied by a number of departments or agencies, where the CBSA is not the major tenant, the most senior CBSA official must:

- participate in the development and/or review of the emergency procedures and evacuation plans;







- recruit volunteers to act as building emergency officer *for the areas occupied by the CBSA;* and,
- communicate with other tenants.

Where more than 50 employees are working in a building at any time, a Building Emergency Organization (BEO) must be established as required by the Canada Labour Code.

In buildings where less than 50 employees work at any given time, one employee along with an assistant must be designated responsible for emergency matters in the building. They will be known as the "Chief Building Emergency Officer" and the "Deputy Chief Building Emergency Officer ", respectively. For example, at smaller Customs Border Crossings, the Chief of Operations and Superintendent would normally hold these responsibilities.

## 3. Building Risk Analysis

The risk analysis lays the foundation for the planning of the Building Emergency Response Plan (BERP).

The Canada Labour Code, Part II, requires employers to make employees aware of every known or foreseeable safety or health hazard in the areas where they work. A risk analysis must be conducted since a key part of emergency response is the awareness and understanding of the environment. This includes an analysis of both internal and external factors, such as building location, as well as assets and emergency services which could impact or influence how an organization responds to and manages an emergency.

## 4. Plan Approval

The Building Emergency Response Plan (BERP) shall be forwarded to the Regional Security Office and in Headquarters to the HQ Security Section for review and the Security and Professional Standards Directorate (SPSD) for acceptance before implementation.

The municipal fire department has the authority to review and accept the fire emergency procedures and evacuation plan for a building.

## 5. Roles and Responsibilities

### 5.1 Building Emergency Organization

The Building Emergency Organization (BEO) is a team of employees, from within the building, which works with the Responsible Building Authority (RBA) during building emergencies. Under the Canada Labour Code, the employer is responsible and accountable for these volunteers while they perform their duties. Although the employee has volunteered for these







additional duties, it is not a normal condition of employment and the employee would therefore still have the right to refuse. It should be noted that other than the RBA, all members of the Building Emergency Organization (BEO) are volunteers and comprise of the following positions:

- Responsible Building Authority (RBA);
- Chief Building Emergency Officer (CBEO);
- Floor Emergency Officer (FEO).

Note that one or multiple deputies could be added to each position.

**5.2 Responsible Building Authority (RBA)**

When a building is fully or primarily occupied by the CBSA, the highest-ranking official is deemed the RBA and is responsible to ensure that the Building Emergency Response Plan (BERP) meets the requirements of this Directive.

The RBA is responsible for:

a) Ensuring that a current BERP exists for the building and that it is fully implemented and administered;
b) Establishing a Building Emergency Organization (BEO);
c) Appointing one (or multiple) Deputy RBA(s);
d) Ensuring that at all times during core business hours, either the RBA or one of the DRBA`s are present and in the building;
e) Ensuring that the BEO members are trained to perform their duties in fire prevention, other emergencies, and emergency evacuation of the building;
f) Ensuring that fire and other emergency drills are held as required;
g) Ensuring that each member of the Building Emergency Organization (BEO) is instructed and trained in their responsibilities;
h) Maintaining proper records of current:
    - BEO members;
    - The number and fire evacuations and other emergency drills;
    - The number fire and emergency incidents in the building;
    - Training and activities provided to BEO members;
    - Dates BEO meetings were held;
    - Mobility Impaired occupants in the building;
    - Risks associated with their building of occupancy.







During an emergency:

The RBA assumes full authority for the emergency response of all building occupants until the emergency is terminated or until the first responders arrive at the scene and assume responsibility. He/she must:

a) Adopt measures, including making on-the-spot decisions for the safety of employees in the building. Examples of such decisions include:
   - to evacuate;
   - to remain on the floor;
   - to determine safe exit routes;
   - to relocate occupants;
b) At all times during an emergency, the RBA must be able to communicate effectively with building tenants. The RBA is responsible to identify and use the most appropriate means of communications to transmit messages to building tenants. Means of communications include: public address system (PA), megaphone, emails, telephone lists, members of the BEO, etc;
c) Notify the Border Operations Centre (BOC) and the Regional Security Office as soon as possible;

If an evacuation of the building occupants is required:

d) Advise the Chief Building Emergency Officer to proceed with the evacuation procedures as indicated in the BERP;
e) When possible, advise the personnel and visitors of the reason and need to evacuate;

If a shelter-in-place of building occupants is required:

f) Advise the Chief Building Emergency Officer to proceed with the shelter-in-place procedures as indicated in the BERP;
g) When possible, advise the personnel and visitors of the reason and need to shelter-in-place;
h) Take steps to ensure no one leaves their respective areas (if required);
i) Maintain communication with the Chief Building Emergency Officer to exchange reports and vital information on the state of the emergency;

Post-emergency:





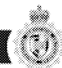


j) Ensure the Occupational Health and Safety Committee and the Regional Security Office or in Headquarters the HQ Security Section complete a visual inspection with the Chief Building Emergency Officer following the activation of the Building Emergency Response Plan;
k) Order re-entry following approval from the first responders;
l) Conduct a debriefing session after each emergency with the building emergency organization members, Occupational Health and Safety Committee representative, and the Regional Security Office or in Headquarters the HQ Security Section;
m) Arrange for the Employee Notice Line to be updated in the event of a building closure.

### 5.3 Chief Building Emergency Officer (CBEO)

The Chief Building Emergency Officer (CBEO) is responsible for:

a) The day-to-day implementation of the BERP (i.e. protection and prevention activities);
b) Preparation, implementation and administration of the BERP (including annual reviews);
c) Ensuring the establishment and continuity of the BEO by recruiting qualified personnel for each floor such as the Floor Emergency Officers (FEO) and Deputy Floor Emergency Officers (DFEO);
d) Advising the RBA, in writing, of any changes in the status of the Chief Building Emergency Officer (CBEO) or the Deputy (ies);
e) Ensuring that there are monitors identified for all mobility impaired persons;
f) Developing an Evacuation Plan including procedures for the safe evacuation of persons requiring assistance;
g) Holding regular meetings with the members of the Emergency Organization and the Occupational Health and Safety Committee;
h) Holding fire and other emergency related drills as required and ensuring that a debriefing session is conducted afterwards;
i) Ensuring, in collaboration with the property manager, that floor layouts showing the type, location and operation of building emergency systems (stairwells, emergency telephones, etc.) are immediately accessible to local authorities (such as the fire department);
j) Ensuring, in collaboration with the property manager, that all necessary keys are properly identified and immediately accessible at all times to local authorities (ex: keys for the mechanical room, keys for elevators);
k) Posting copies of all emergency instructions (i.e. Fire, Bomb threat procedures) at a conspicuous location on each floor;



l) Ensuring the Emergency Organization is properly equipped to handle emergencies (i.e. personal copy of emergency plans/procedures, flashlights, caps, megaphones etc.);
m) Reporting false alarms and/or building faulty conditions to the Property Manager;
n) Liaising with responsible authorities such as the fire department, police and building management during an emergency;
o) Establishing relationships with Chief Building Emergency Officers of neighbouring buildings in order for mutual assistance to be pre-planned (i.e. shelter occupants during inclement weather, First Aid assistance);
p) Supervising search procedures and/or evacuation procedures at time of a building evacuation and liaising with first responders and building authorities;
q) Ensuring that the CBEO or the DCBEO is always present in the building.
r) Ensuring the Building Emergency Organization (BEO) has current contact lists and telephone numbers (i.e. laminated cards);
s) If applicable, ensuring the Security Guard Post has a current contact list of members of the Emergency Organization and that all emergency equipment at the guard post(s) is maintained in good condition.

During an emergency:

t) Make certain that local authorities have been notified;
u) Meet Emergency Services when they arrive and provide any keys and floor layout drawings required;
v) Ensure that each floor or special area is completely evacuated;
w) Wait for instructions from the Officer-in-charge with the local authorities before allowing people to re-enter the building; and,
x) Take steps to ensure no one re-enters the building.

**5.4 Floor Emergency Officers (FEO) and Deputy Floor Emergency Office (DFEO)**

The FEO and DFEO are responsible for:

a) Ensuring the safety of all personnel, including visitors on their floor in the event of an emergency during the buildings core business hours;
b) Notifying the CBEO of all emergencies;
c) Appointing monitors to assist mobility impaired persons;
d) Arranging for a replacement to cover their duties in case they are absent.
e) Advising the CBEO of the location of the mobility-impaired persons and their assigned monitor;
f) Being familiar with the emergency procedures in this plan;





g) Ensuring that defective or damaged tools are reported to the CBEO. Examples include but are not limited to:
   - Exit lights out;
   - Firefighting equipment inoperative or obstructed;
   - Fire doors blocked open or wedged.

During an evacuation:

h) Closing fire and smoke doors, when possible;
i) Ensuring that all occupants on their floor evacuate the building;
j) Ensuring assigned Monitors are available to help all mobility-impaired persons to evacuate the building;
k) Ensuring that individuals do not operate elevators unless the local authorities specifically authorize you to do so;
l) As soon as the evacuation flow is over, checking all rooms, closets and washrooms to ensure that the floor is completely evacuated;
m) Upon complete evacuation, regrouping with the other officers and leaving together;
n) Report the status of the evacuation to the Chief Building Emergency Officer.

## 5.5 Responsibilities of All Building Occupants

All occupants are responsible for:

a) Familiarizing themselves with the BERP and procedures to be followed in the event of a fire or other emergency;
b) Their personal safety;
c) Ensuring that visitors follow the same evacuation orders;
d) ) Any person seeing Fire, or Smoke, or smelling a noxious gas is to:
   - Pull the nearest fire alarm station;
   - Warn persons nearby; and
   - Telephone the Fire Department from the nearest safe location.
e) Evacuate immediately using the predetermined safe exit and proceed outside. Move away from the building to a minimum of 100m and meet at the predetermined meeting place.
f) Refrain from using elevators for evacuation purposes.

## 5.6 Persons Requiring Assistance



Many CBSA employees or clients could require additional assistance during an emergency evacuation. For emergency planning purposes, mobility-impairment is a physical or medical disability which, even with the aid of monitors, would prevent that person from descending the stairs. For example, in an evacuation situation at a rate of speed consistent with the normal flow of other building occupants, or which would cause such person physical harm if they attempted to descend the stairs. Examples include but are not limited to:

- People who have mobility or other activity limitations (e.g. due to respiratory or cardiac conditions, reduced stamina, joint pain, etc.);
- Employees who have diminished or hearing loss;
- Employees who are blind or visually impaired;
- Employees who have claustrophobia, fear of heights or fear of crowds;
- Employees who have sustained a recent injury (e.g. broken leg, broken foot, etc.) or have temporary limitations due to surgery, accidents, pregnancy or injuries.

Any occupant who requires special assistance in evacuating the building is responsible for:

a) Advising his/her Floor Emergency Officer of their location on the floor and the assistance required including the type and location of any special equipment or aide the individual requires;
b) Assisting the Floor Emergency Officer in appointing his/her monitors.

The plan for the safe evacuation of employees who require special assistance shall be established in consultation with those employees and their assigned monitors. This consultation can take place one-on-one or in small groups, if for any reason the person requiring assistance is unable to attend plenary meetings of the Building Emergency Organization, provided that:

(i) The person meets with a member of the BEO once a year to review their evacuation plan as required by the Canada Labour Code;

(ii) They meet with the same member of the BEO (barring personnel changes) to ensure continuity, and,

(iii) A record is kept on file of this meeting and the results of it.

Unless specifically exempted, the individual and their assigned monitors should participate in an evacuation exercise, in order to familiarize themselves with the procedures and to ensure a safe evacuation in a real event.

During an Alarm, Core Business Hours:







When the alarm sounds during regular business hours:

a) Persons requiring assistance and their Monitors are to go directly to the pre-determined designated safe location within the floor area;
b) Persons requiring assistance are advised to remain on their floor area in the designated safe location until the arrival of local authorities, unless they are in immediate danger (ex: on the floor where the fire started);
c) After the initial flow of the evacuees has diminished, the Monitors may proceed to evacuate the persons requiring assistance down the stairwell (for example) to the exterior of the building, if it is safe to do so;
d) In all situations, the FEO will report to the CBEO when the evacuation of the floor is completed or if assistance is required;
e) If for any reason the evacuation of the person requiring assistance has to be put on hold and the Monitor and person requiring assistance need to take refuge on a floor other than their own, the FEO will notify the CBEO of their location. This can be done by advising other evacuees as they proceed to evacuate the building, by using the telephone, or by waving and shouting from a window to alert emergency services and/or bystanders
f) Once evacuated, Monitor and person requiring assistance do NOT re-enter the building until the CBEO has given permission to do so;

Outside of Core Business Hours, the persons requiring assistance must:

g) Inform their immediate supervisor, the FEO or the DFEO of their plans as well as the date and time that they will be in the building;
h) If planning on working outside of core business hours, the persons requiring assistance are responsible for the following:
    - Identifying an evacuation plan in advance of working outside of the core business hours. This entails identifying if monitors will be available.

When the alarm sounds outside of Core Business Hours, the persons requiring assistance must:

i) Follow the plan that was developed prior to working outside of the core business hours;
j) In the absence of a plan, contact Emergency Services to specify their exact location; and,
k) Follow the instructions provided, based on the situation.







## 5.7 Monitors

Upon hearing an alarm, Monitors are responsible for:

a) Meeting with the person requiring assistance to a pre-arranged location on the floor area (but not blocking evacuation traffic);
b) Evacuating the person requiring assistance to the exterior of the building when it is safe to do so.

## 5.8 Occupational Health and Safety Committee

Occupational Health and Safety Committee or representative must:

a) Be consulted in the development and review of emergency procedures;
b) Be notified of all emergency situations; and,
c) Participate in the investigation, in accordance with their local Terms of Reference.

## 5.9 Agency Building Official (ABO)

When the Agency is a minor tenant in a building, the Agency Building Official (ABO) also called Senior Official, must work in collaboration with the major federal tenant or the building owner to ensure that the Building Emergency Response Plan satisfies the requirements of this Directive for the space CBSA occupies.

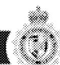
The ABO is responsible for:

- Assigning a Deputy Agency Building Official (DABO);
- Ensuring that each area occupied by the Agency has floor emergency officers and deputies identified;
- Providing emergency preparedness awareness sessions to Agency employees;
- Ensuring the Agency is represented in the building emergency organization; and,
- Participating in building emergency organization activities;

During an emergency:







- The Responsible Building Authority (RBA) of the major tenant organization assumes full authority for the emergency response of all building occupants until the emergency is terminated or until the first responders arrive at the scene and assume responsibility;
- Although the RBA has full authority, the ABO must ensure that actions taken during an emergency are in the best interest of the health and safety of CBSA employees;
- The ABO's responsibilities during an emergency will be determined by the RBA and the position the ABO holds on the building emergency organization;

Following an emergency:

The ABO must:

- Coordinate re-entry with the RBA;
- Notify the Border Operations Centre (BOC) and the Regional Security Office or in Headquarters the HQ Security Section, if the emergency has affected an area occupied by the Agency;
  Arrange for the Employee Notice Line to be updated in the event of a building closure.

### 5.10 Physical Security Section, Security and Professional Standards Directorate (SPSD)

The Physical Security Section, from the Security and Professional Standards Directorate (SPSD) will provide technical support to Operations on a case by case basis with respect to asset protection and security issues on a case by case basis considering the impacts may vary based on the emergency.

## 6. Equipment for Building Emergency Organization Members

Each employer must purchase the necessary equipment for its own employees who are members of the emergency organization.

All members of the emergency organization must be clearly and distinctively identified (coloured hardhat and/or vest, etc.). Distinctive colours must be used to clearly and separately identify the Chief Building Emergency Officer, the Deputy Chief Building Emergency Officer, Floor Emergency Officers and monitors.

In all buildings flashlights must be provided to each member of the BEO and must be maintained in good operating condition.

Due to building configurations, buildings occupied by 100 or more occupants must possess a battery-operated portable loudspeaker to assist with crowd control.







## 7. Fire Protection and Other Equipment

Building owners, Property Managers, or PWGSC in lease buildings, must ensure that all emergency equipment is installed, inspected and maintained in accordance with the applicable standards or regulations.

## 8. Evacuation Drills

There must be at least one total building evacuation drill each year involving all occupants in the building. Whereas partial drills are considered useful to supplement the complete evacuation drill, they should not replace it. A record of each drill in the building must be kept for a period of 2 years from the date of the drill.

The local fire department should be contacted in advance to establish the notification schedule and procedures prior to any fire alarm system activation for the purpose of carrying out a drill. This notification is generally required at least one week in advance if fire department participation is desired during a drill, and immediately prior to any fire alarm system activation and afterwards as soon as the fire alarm system has been restored to normal operating condition.

In multi-occupancy buildings where the CBSA is not the main tenant, the Agency Building Official (ABO) or the Senior Official should make every reasonable effort to coordinate a yearly evacuation drill with the other occupants of the building. In the event that such efforts are not successful, the Regional Security Office or in Headquarters the HQ Security Section, should be contacted for assistance.

## 9. Emergency Plans Other than Fire Evacuation Plans

Emergency plans, other than fire evacuation plans, must be tested at least every two years. Tabletop exercises are an effective means of evaluating a plan. More information on how to conduct a tabletop exercise can be obtained from SPSD.

## 10. Reporting Requirements

All incidents relating to this chapter must be reported to your Regional Security Office or in Headquarters the HQ Security Section, and to the SPSD, by filling a security incident report (form BSF152).

All incidents that relate to the Incident Reporting Criteria are to be reported to the Border Operations Center (BOC) by phone at 613-960-6001, or by email at: boc-cof@cbsa-asfc.gc.ca.

## 11. Training of Building Emergency Organization

Every member of the Building Emergency Organization (BEO) must be instructed and trained in their responsibilities under the emergency plan and in the use of fire protection equipment, as applicable. Training should include meetings, viewing of films or videotapes, presentations







by guest speakers, training courses and participation in Fire Prevention Week and Emergency Preparedness Week activities. Guest speakers can be invited from the local fire department or private companies. Extinguisher or other training courses are offered by local fire departments or by recognized companies involved in security and safety. The Regional Security Advisor and/or the Security and Professional Standards Directorate (SPSD) should be consulted for assistance.

A record of all instruction and training provided to the BEO must be kept for a period of two (2) years from the date in which the instruction and training was provided.

All of the BEO members must be given a copy of the Emergency Plan prepared for their building.

The Chief Building Emergency Officer must conduct meetings, at least once a year and after any change is made in the policy, Emergency Evacuation Plan or the Emergency Procedures for the building, to inform members of the Emergency Organization of emergency planning issues; discuss concerns; and update the lists of emergency organization members and of persons requiring assistance.

The Chief Building Emergency Officer must keep a record of each meeting for a period of two years from the date of the meeting. The record must contain the date of the meeting, the names and titles of those present and a summary of the matters discussed.

The Chief Building Officer must keep a record of each drill for a period of two years from the date of drill. The record must include the date and time of the drill and where applicable, the length of time taken to evacuate the building.

## 12. Employee Training

Local management with the assistance of the local Occupational Health and Safety (OHS) should determine the nature and scope of instruction and training needed in the workplace. The extent and depth of the training depends on the hazards particular to the workplace.

Local management must ensure that instructions for employees to follow in case of an emergency, including evacuation, are posted at appropriate locations and that employees are aware of emergency measures and procedures.

Training can be provided through lectures, films, hands-on demonstrations, information brochures or pamphlets, etc.

## 13. CBSA Employee Notice Line

The CBSA Employee Notice Line 1-866-NOTICE4 (1-866-668-4234) is to be used for getting up-to-date information about the workplace in the event of a building closure. Examples of







emergency or disruption to regular operations are inclement weather, environmental disasters, local or national emergencies, demonstrations and building occupations.

## 14. CBSA Employee Assistance Program (EAP)

Critical Incident Stress debriefings provide a forum in which personnel can discuss their feelings and reactions as a result of a stressful incident. The support and assistance of the CBSA Employee Assistance Program (EAP) services are available to employees to ensure their continued well-being following any traumatic event. Following any such incidents, the Occupational Health and Safety Committee in the affected area is encouraged to advise managers of the requirement for a critical incident stress debriefing for employees. Managers will contact Human Resources for assistance.

## 15. Inspections

A visual inspection must be carried out by a qualified person (a municipal official or a technically competent supplier of emergency equipment) at least every 6 months and must include an inspection of all fire escapes, exits, stairways and fire protection and other emergency equipment in the building in order to ensure that all are in serviceable condition and are ready for use at all times.

A record of each inspection must be dated and signed by the person who carried out the inspection. It must also be kept in the building, to which it applies, by the Chief Building Emergency Officer for a period of two years from the date in which it is signed.

Members of the emergency organization must report any obvious faulty conditions discovered during routine or daily visual inspections to the appropriate official for corrective action. Faulty conditions include: fire doors wedged or blocked open; exits, stairways and corridors obstructed; exit lights out; firefighting equipment inoperative or obstructed; and obvious hazards such as the unnecessary accumulation of combustibles, the improper use of flammable liquids, temporary or unsafe electric wiring and other unsafe conditions and practices.







# Annexe A : Directive concernant la planification des interventions d'urgence dans les immeubles

## 1. Introduction

Le présent document fournit les procédures et les lignes directrices nécessaires à l'élaboration de plans d'urgence et à la mise sur pied d'organismes de secours efficaces. Un modèle détaillé d'un plan d'intervention d'urgence de l'immeuble (PIUI) est présenté à l'annexe A. Il contient des renseignements et des éléments essentiels qui devraient être inclus dans les plans d'urgence. Pour des renseignements propres aux différentes catégories de menace, prière de se reporter aux annexes pertinentes.

L'élaboration et l'examen de tous les plans d'intervention d'urgence de l'immeuble doivent faire l'objet d'une démarche coordonnée entre divers partenaires. Ces derniers comprennent entre autres :

- le comité de santé et de sécurité au travail;
- les autres locataires de l'immeuble et les autres ministères;
- les gestionnaires immobiliers;
- les gestionnaires immobiliers des immeubles voisins;
- les coordonnateurs des services d'urgence municipaux (services de police, services des incendies, équipes d'intervention en présence de matières dangereuses, etc.);
- les services municipaux de santé publique;
- l'administration des ponts, l'administration aéroportuaire;
- les courtiers;
- les douanes américaines.

## 2. Responsabilités liées à l'élaboration et à l'administration du plan d'intervention d'urgence de l'immeuble

Dans les immeubles occupés exclusivement ou principalement par des employés de l'Agence des services frontaliers du Canada (ASFC), le plus haut fonctionnaire de l'ASFC dans l'immeuble est considéré comme l'autorité responsable de l'immeuble (ARI). À ce titre, il doit veiller à ce que les plans d'urgence soient élaborés et mis à jour.

Dans les immeubles occupés par un certain nombre de ministères ou d'organismes (c'est-à-dire que l'ASFC n'en est pas le locataire principal), le plus haut fonctionnaire de l'ASFC dans l'immeuble doit :







- participer à l'élaboration et/ou à l'examen des procédures d'urgence et des plans d'évacuation;
- recruter des volontaires en mesure de jouer un rôle d'agent de secours de l'immeuble dans les *zones occupées par l'ASFC*;
- communiquer avec les autres locataires.

Dans les immeubles où travaillent, en tout temps, plus de 50 employés, il faut former un Organisme de secours de l'immeuble (OSI) conformément au *Code canadien du travail.*

Dans les immeubles où travaillent, en tout temps, moins de 50 personnes, un employé et son assistant doivent être chargés des questions liées aux interventions d'urgence propres à l'immeuble. Cet employé et son assistant sont appelés respectivement « agent de secours en chef de l'immeuble (ASCI) » et « adjoint de l'agent de secours en chef de l'immeuble (AASCI) ». Par exemple, dans les petits postes frontaliers, le chef des opérations et le surintendant assumeraient normalement ces responsabilités.

## 3. Analyse des risques liés à l'immeuble

La préparation du plan d'intervention d'urgence de l'immeuble (PIUI) repose sur une analyse des risques.

Le *Code canadien du travail*, partie II, exige que les employeurs veillent à ce que soient portés à l'attention de chaque employé les risques connus ou prévisibles que présente pour sa santé et sa sécurité l'endroit où il travaille. Une analyse des risques doit être menée, car la connaissance et la conscience de l'environnement sont des éléments clés de l'intervention d'urgence. Une telle analyse comprend une analyse des facteurs internes et externes – l'emplacement de l'immeuble, par exemple – ainsi que de l'équipement et des services d'urgence susceptibles d'influer sur la manière dont un organisme interviendra dans une situation d'urgence et la gérera.

## 4. Approbation du plan

Le plan d'intervention d'urgence de l'immeuble (PIUI) doit être transmis au Bureau régional de la sécurité et pour l'Administration centrale, à la Section de la sécurité de l'AC, pour revue, et à la Direction de la sécurité et des normes professionnelles (DSNP) pour approbation avant sa mise en œuvre.

Le service municipal des incendies a le pouvoir d'examiner et d'accepter les procédures d'urgence-incendie et le plan d'évacuation pour un immeuble.







## 5. Rôles et responsabilités

### 5.1 Organisme de secours de l'immeuble

L'Organisme de secours de l'immeuble est formé d'une équipe d'employés de l'immeuble qui collabore avec l'autorité responsable de l'immeuble (ARI) durant les situations d'urgence. En vertu du *Code canadien du travail*, l'employeur est responsable de ces bénévoles pendant qu'ils s'acquittent des tâches qui leur sont assignées. Un employé peut refuser de s'acquitter de ces tâches, car elles ne font pas partie de celles dont il doit s'acquitter normalement dans le cadre de ses fonctions. Il convient de noter que, mis à part l'ARI, tous les membres de l'Organisme de secours de l'immeuble (OSI) sont des bénévoles. Les postes de l'OSI sont les suivants :

- l'autorité responsable de l'immeuble (ARI);
- l'agent de secours en chef de l'immeuble (ASCI);
- l'agent de secours d'étage (ASE).

Remarquez qu'un ou plusieurs adjoints peuvent se greffer à chaque poste.

### 5.2 Autorité responsable de l'immeuble (ARI)

Lorsqu'un immeuble est entièrement ou principalement occupé par l'ACSF, le plus haut fonctionnaire de l'ACSF dans l'immeuble est désigné à titre d'ARI et doit s'assurer que le plan d'intervention d'urgence de l'immeuble (PIUI) satisfait aux exigences de la présente directive.

L'ARI doit :

a) s'assurer qu'un PIUI est en vigueur et qu'il est intégralement appliqué et administré;
b) établir un organisme de secours de l'immeuble (OSI);
c) nommer un adjoint de l'autorité responsable de l'immeuble (AARI) ou plusieurs;
d) veiller à ce que, en tout temps durant les heures de travail normales, une ARI ou l'un des AARI soit présent dans l'immeuble;
e) s'assurer que les membres de l'OSI ont reçu une formation sur la prévention des incendies, sur d'autres types d'interventions d'urgence et sur les procédures d'évacuation d'un immeuble en cas d'urgence;
f) s'assurer que des exercices d'évacuation en cas d'incendie ou des exercices d'alerte ont lieu comme requis;
g) s'assurer que chaque membre de l'Organisme de secours de l'immeuble (OSI) reçoit la formation nécessaire et connaît ses responsabilités;







h) tenir des dossiers appropriés en ce qui concerne :
   - les membres de l'OSI;
   - le nombre d'exercices d'évacuation en cas d'incendie ou d'autres exercices d'alerte;
   - le nombre des incendies ou d'autres incidents survenus dans l'immeuble;
   - la formation et les activités offertes aux membres de l'OSI;
   - les dates auxquelles les réunions de l'OSI ont eu lieu;
   - les occupants à mobilité réduite de l'immeuble;
   - les risques associés à l'usage de l'immeuble;
   - la formation sur les risques associés à l'immeuble offerte aux membres de l'OSI (pour connaître ces risques, il suffit de communiquer avec le Bureau régional des services et les autorités locales).

Pendant une urgence

L'ARI assume l'entière responsabilité de l'intervention d'urgence menée auprès de tous les occupants de l'immeuble tant que l'urgence n'a pas pris fin ou que les premiers intervenants ne sont pas arrivés sur les lieux pour prendre en charge l'intervention.

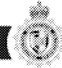
L'ARI doit :

a) adopter des mesures, y compris prendre des décisions rapides pour assurer la sécurité des employés se trouvant dans le bâtiment, notamment celles :
   - de procéder à l'évacuation,
   - de demander aux occupants de rester à l'étage,
   - d'établir des issues de sortie sécuritaires,
   - de relocaliser les occupants;
b) en tout temps lors d'une situation d'urgence, pouvoir communiquer efficacement avec tous les locataires de l'immeuble. L'ARI est responsable d'identifier et d'utiliser des moyens de communication pour transmettre des messages aux locataires. Ces moyens de communication incluent des systèmes de diffusion publique, des mégaphones, des courriels, des listes de téléphone, l'utilisation des membres de l'organisme de secours de l'immeuble, etc.;
c) avertir le Centre des opérations frontalières (COF) et le Bureau régional de la sécurité le plus rapidement possible.

Si l'évacuation des occupants de l'immeuble est requise, l'ARI doit :







d) demander à l'agent de secours en chef de l'immeuble (ASCI) de mettre en œuvre les procédures d'évacuation prévues dans le PIUI;
e) dans la mesure du possible, expliquer au personnel et aux visiteurs qu'ils doivent évacuer et pourquoi ils doivent le faire.

Si le regroupement des occupants de l'immeuble dans un abri sur place est nécessaire, l'ARI doit :

f) demander à l'agent de secours en chef de l'immeuble (ASCI) de mettre en œuvre les procédures d'évacuation prévues dans le PIUI;
g) dans la mesure du possible, expliquer au personnel et aux visiteurs qu'ils doivent se regrouper dans un abri sur place et pourquoi ils doivent le faire;
h) prendre des mesures pour que personne ne quitte son abri sur place respectif (le cas échéant);
i) rester en communication avec l'agent de secours en chef de l'immeuble (ASCI) en échangeant des rapports et des renseignements vitaux sur la situation d'urgence.

Après la situation d'urgence, l'ARI doit :

j) s'assurer que le comité de santé et de sécurité au travail et le Bureau régional de la sécurité ou pour l'Administration centrale, la Section de la sécurité de l'AC, effectuent une inspection visuelle avec l'agent de secours en chef de l'immeuble (ASCI) après la mise en œuvre du plan d'intervention d'urgence de l'immeuble (PIUI);
k) ordonner le retour dans l'immeuble des personnes évacuées après avoir reçu l'approbation des premiers intervenants;
l) mener une brève séance d'information après chaque urgence avec les membres de l'Organisme de secours de l'immeuble (OSI), le représentant du comité de santé et de sécurité au travail et le Bureau régional de la sécurité ou pour l'Administration centrale, la Section de la sécurité de l'AC;
m) veiller à ce que la ligne d'information des employés soit mise à jour en cas de fermeture de l'immeuble.







### 5.3 Agent de secours en chef de l'immeuble (ASCI)

L'agent de secours en chef de l'immeuble (ASCI) doit :

a) veiller à la mise en œuvre des activités quotidiennes prévues au PIUI (c.-à-d. les activités de protection et de prévention);
b) préparer, mettre en œuvre et administrer le PIUI (y compris les examens annuels du PIUI);
c) veiller à créer l'Organisme de secours de l'immeuble et à en assurer la continuité en recrutant des employés qualifiés pour chaque étage, comme des agents de secours d'étage (ASE) et des adjoints des agents de secours d'étage (AASE);
d) informer l'ARI, par écrit, de tout changement concernant le statut de l'agent de secours en chef de l'immeuble (ASCI), de son adjoint ou de ses adjoints;
e) nommer des accompagnateurs désignés pour aider les personnes à mobilité réduite;
f) élaborer un plan d'évacuation, y compris des procédures pour l'évacuation sans danger des personnes ayant besoin d'aide;
g) tenir régulièrement des réunions avec les membres de l'Organisme de secours de l'immeuble et du comité de santé et de sécurité au travail;
h) tenir des exercices d'évacuation en cas d'incendie et d'autres exercices d'alerte connexes (tel que requis) et s'assurer que des séances de rétroaction ont lieu après ces exercices;
i) en collaboration avec le gestionnaire de l'installation, s'assurer que les autorités locales (comme le service d'incendie) puissent avoir immédiatement accès aux plans d'étage indiquant le type, l'emplacement et le fonctionnement des systèmes d'urgence de l'immeuble (cages d'escalier, téléphones d'urgence, etc.);
j) en collaboration avec le gestionnaire de l'installation, veiller à ce que toutes les clés dont les autorités locales pourraient avoir besoin (p. ex., les clés des locaux techniques, des ascenseurs) soient identifiées de manière appropriée et accessibles immédiatement en tout temps;
k) afficher des copies de toutes les instructions ayant trait aux mesures d'urgence (c.-à-d. incendie, alerte à la bombe) dans un endroit bien en vue à chaque étage;
l) s'assurer que les membres de l'Organisme de secours de l'immeuble (OSI) sont convenablement équipés pour faire face à une urgence (copie personnelle des plans et des procédures d'urgence, lampes de poche, casques, mégaphones, etc.).
m) signaler les fausses alarmes et/ou les conditions défectueuses de l'immeuble au gestionnaire immobilier;







n) assurer la liaison avec les autorités responsables comme le service incendie, le service de police et la direction de l'immeuble durant une urgence;
o) demeurer en liaison avec ses homologues d'immeubles voisins afin que les services d'assistance mutuelle soient planifiés (p. ex., abriter les occupants durant les intempéries, fournir les premiers secours);
p) superviser les procédures de recherche et/ou d'évacuation et assurer la liaison avec les premiers intervenants et les responsables de l'immeuble;
q) s'assurer que l'ASCI ou l'AASCI est toujours présent dans l'immeuble;
r) s'assurer que l'Organisme de secours de l'immeuble (OSI) possède des listes à jour des noms et numéros de téléphone de ses membres (c.-à-d. cartes laminées);
s) s'il y a lieu, s'assurer que le préposé au poste de garde de sécurité possède une liste à jour des membres de l'Organisme de secours de l'immeuble (OSI) et que tout le matériel d'urgence se trouvant au poste de garde de sécurité est maintenu en bon état.

Pendant l'urgence, l'ASCI doit :

t) s'assurer que l'on a averti les premiers intervenants;
u) aller à la rencontre des membres du service d'urgence à leur arrivée et leur remettre les clés et les plans des étages, au besoin;
v) s'assurer que chaque étage ou zone spéciale est complètement évacué;
w) attendre les directives du responsable des autorités locales avant de permettre aux occupants de retourner dans l'immeuble;
x) prendre des mesures afin que personne ne retourne dans l'immeuble.

## 5.4 Agent de secours d'étage (ASE) et adjoint de l'agent de secours d'étage (AASE)

L'ASE et l'AASE doivent :

a) assurer la sécurité de tout le personnel ainsi que des visiteurs se trouvant à leur étage s'il survient un incendie ou une autre situation d'urgence pendant les heures de travail normales des employés de l'immeuble;
b) informer l'ASCI de toute situation d'urgence;
c) nommer des accompagnateurs pour aider les personnes à mobilité réduite;
d) désigner une personne qui pourra les remplacer en leur absence;
e) informer l'ASCI de l'endroit où se trouvent les personnes à mobilité réduite et leur accompagnateur désigné;
f) connaître les procédures d'urgence décrites dans le présent plan;





g) s'assurer que les outils défectueux ou endommagés sont signalés à l'ASCI, y compris :
   - des sorties de secours qui ne sont pas éclairées;
   - un équipement de lutte contre les incendies non fonctionnel ou obstrué;
   - des portes coupe-feu bloquées en position ouverte ou entre-ouvertes.

Durant une évacuation, l'ASE et l'AASE doivent :

h) fermer les portes coupe-feu et les cheminées d'appel, si possible;
i) s'assurer que tous les occupants sur leur étage sortent de l'immeuble;
j) s'assurer que des accompagnateurs désignés sont disponibles pour aider les personnes à mobilité réduite à sortir de l'immeuble;
k) s'assurer que les personnes n'utilisent pas les ascenseurs, à moins que les autorités locales aient donné une autorisation précise en ce sens;
l) dès que la majorité du personnel est évacuée, s'assurer que toutes les pièces, les placards et les toilettes ont été complètement évacués;
m) une fois l'évacuation terminée, se joindre aux autres agents et sortir avec eux;
n) faire rapport du statut de l'évacuation à l'agent de secours en chef de l'immeuble (ASCI).

**5.5. Responsabilités de chaque occupant de l'immeuble**

Tous les occupants doivent :

a) bien connaître le PIUI et les consignes à suivre en cas d'incendie ou de toute autre situation d'urgence;
b) veiller à sa propre sécurité;
c) s'assurer que les visiteurs suivent les mêmes consignes d'évacuation qu'eux;
d) s'ils aperçoivent des flammes/de la fumée ou sentent une odeur du gaz :
   - déclencher l'avertisseur d'incendie le plus près;
   - avertir les personnes se trouvant dans leur environnement immédiat;
   - appeler le service d'incendie à partir du lieu sûr le plus proche;
e) évacuer les lieux immédiatement en empruntant l'issue sûre préétablie et se rendre à l'extérieur; s'éloigner d'au moins 100 m de l'immeuble vers un lieu de rassemblement prédéterminé;
f) éviter d'utiliser les ascenseurs pour l'évacuation.



## 5.6 Personnes ayant besoin d'aide

Beaucoup d'employés ou de clients de l'ASFC pourraient avoir besoin d'une aide supplémentaire durant une évacuation d'urgence. Aux fins de l'établissement des plans d'urgence, une personne ayant besoin d'aide est définie comme une personne à mobilité réduite (PMR) dont l'état physique ou médical, même en la présence d'un accompagnateur, l'empêcherait lors d'une évacuation d'urgence de descendre les escaliers à la cadence normalement soutenue par les autres occupants de l'immeuble ou serait aggravé du seul fait de tenter de descendre les escaliers. Parmi ces personnes, mentionnons, entre autres :

- les gens dont la mobilité ou d'autres activités sont limitées (à cause, par exemple, de problèmes respiratoires ou cardiaques, d'une faible endurance, de douleurs articulaires, etc.);
- les employés qui souffrent d'une atténuation ou d'une perte d'audition;
- les employés aveugles ou qui souffrent d'une déficience visuelle;
- les employés qui souffrent de claustrophobie, de vertige ou de crainte excessive des foules;
- les employés victimes d'une blessure récente (fracture d'une jambe ou d'un pied, etc.) ou dont les mouvements sont temporairement limités à cause d'une chirurgie, d'un accident, d'une grossesse ou de certaines blessures).

Tout occupant qui a besoin d'une aide spéciale pour évacuer l'immeuble doit :

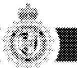
a) indiquer à son agent de secours d'étage (ASE) l'endroit où il travaille sur l'étage et l'assistance dont il a besoin, y compris le type et l'emplacement de tout matériel spécial ou de toute aide précise dont il a besoin;
b) aider l'agent de secours d'étage (ASE) dans la désignation de son ou de ses accompagnateurs.

Le plan d'évacuation sécuritaire des employés ayant besoin d'une aide spéciale doit être établi en consultation avec ces employés et leurs accompagnateurs désignés. Si, pour une raison ou une autre, la personne ayant besoin d'aide n'est pas en mesure d'assister aux assemblées plénières de l'Organisme de secours de l'immeuble (OSI), une consultation individuelle ou en petits groupes peut avoir lieu à condition :

(i) que la personne concernée rencontre un membre de l'OSE une fois l'an afin de revoir son plan d'évacuation, comme l'exige le *Code canadien du travail*;







(ii) que cette personne rencontre le même membre de l'OSE (sauf en cas de changement de personnel) d'année en année afin de garantir la continuité;

(iii) que cette rencontre (et ses résultats) fasse l'objet d'un compte rendu conservé dans un dossier.

À moins d'une exonération spéciale, a personne concernée et ses accompagnateurs doivent participer à un exercice d'évacuation visant à leur permettre de se familiariser avec les procédures et de savoir quoi faire pour sortir sans danger de l'immeuble advenant une situation d'urgence réelle.

Lorsque l'alarme d'urgence est déclenchée pendant les heures de travail normales :

a) les personnes ayant besoin d'aide et leurs accompagnateurs doivent se rendre directement vers un endroit sécuritaire sur l'étage;
b) les personnes ayant besoin d'aide doivent savoir qu'elles doivent rester sur leur étage dans l'endroit sécuritaire désigné jusqu'à l'arrivée des autorités locales, à moins qu'elles ne soient dans une zone de danger immédiat (p. ex., sur l'étage où l'incendie a pris naissance);
c) une fois que la majeure partie des occupants a quitté les lieux, les accompagnateurs peuvent aider les personnes à mobilité réduite à sortir de l'immeuble par l'escalier (par exemple), s'il est possible de le faire sans danger;
d) dans toutes les situations, l'ASE doit indiquer à l'ASCI quand l'évacuation de l'étage est terminée ou si une assistance est requise;
e) si, pour une raison ou une autre, l'évacuation de la personne ayant besoin d'aide est interrompue ou que l'accompagnateur et la personne ayant besoin d'aide doivent se réfugier sur un étage autre que le leur, l'ASE doit aviser l'ASCI de l'endroit où se trouvent la personne ayant besoin d'aide et son accompagnateur (il peut également indiquer cet endroit aux autres personnes en cours d'évacuation, téléphoner ou crier/gesticuler à une fenêtre afin d'alerter les services d'urgence ou des spectateurs);
f) une fois évacués, l'accompagnateur et la personne ayant besoin d'aide NE DOIVENT PAS retourner dans l'immeuble tant que l'ASCI ne leur a pas permis de le faire.

Les personnes ayant besoin d'aide en dehors des heures de travail normales doivent :

g) informer leur superviseur immédiat, l'ASE ou l'AASE de leurs plans ainsi que de la date et de l'heure où elles seront dans l'immeuble;
h) prendre les mesures exposées au point i) ci-après si elles prévoient de travailler en dehors des heures de travail normales;







i) établir un plan d'évacuation avant de travailler en dehors des heures de travail normales (p. ex. indiquer si des accompagnateurs seront disponibles).

Lorsque l'alarme d'urgence est déclenchée en dehors des heures de travail normales, les personnes ayant besoin d'aide doivent :

j) suivre le plan qu'elles ont élaboré avant de travailler en dehors des heures de travail normales;
k) en l'absence d'un plan, communiquer avec les services d'urgence pour indiquer leur emplacement exact;
l) suivre les directives fournies, compte tenu de la situation.

### 5.7 Accompagnateur

Lorsque l'alarme d'urgence est déclenchée, les accompagnateurs doivent :

a) rencontrer la personne ayant besoin d'aide à un endroit prédéterminé sur l'étage (sans bloquer la circulation des personnes en cours d'évacuation);
b) évacuer la personne ayant besoin d'aide à l'extérieur de l'immeuble lorsqu'il est sécuritaire de le faire.

### 5.8 Comité de santé et de sécurité au travail

Le comité de santé et de sécurité au travail ou son représentant doit :

a) être consulté lors de l'élaboration et de l'examen des procédures d'urgence;
b) être avisé de toutes les situations d'urgence;
c) participer aux enquêtes, conformément à son mandat local.



## 5.9 Agent de secours de l'Agence (ASA)

Lorsque l'ACSF n'est pas le locataire principal de l'immeuble, l'agent de secours de l'Agence (ASA), aussi appelé représentant officiel de l'Agence, doit s'assurer, en collaboration avec le locataire principal du gouvernement fédéral ou le propriétaire de l'immeuble, que le plan d'intervention d'urgence de l'immeuble (PIUI) répond aux exigences de la présente directive en ce qui a trait aux locaux occupés par l'ACSF.

L'ASA doit :

- désigner un adjoint, qui est appelé adjoint de l'agent de secours de l'Agence (AASA);
- s'assurer que des agents de secours de l'Agence et leurs adjoints ont été identifiés pour chaque zone occupée par l'ACSF;
- offrir des séances de sensibilisation sur la préparation aux situations d'urgence aux employés de l'ACSF;
- s'assurer que l'ACSF est représentée au sein de l'Organisme de secours de l'immeuble (OSI);
- participer aux activités de l'Organisme de secours de l'immeuble (OIE).

Pendant la situation d'urgence

- L'autorité responsable de l'immeuble (ARI) relevant du locataire principal assume l'entière responsabilité de l'intervention d'urgence auprès de tous les occupants de l'immeuble tant que l'urgence n'a pas pris fin ou que les premiers intervenants ne sont pas arrivés sur les lieux pour se charger de l'intervention.
- Bien que l'ARI relevant du locataire principal assume l'entière responsabilité de la situation, l'ASA doit s'assurer que les mesures prises durant une situation d'urgence sont dans l'intérêt supérieur de la santé et de la sécurité des employés de l'ACSF.
- C'est l'ARI qui détermine les responsabilités de l'ASA durant une situation d'urgence ainsi que la position de l'ASA au sein de l'Organisme de secours de l'immeuble (OSI).

Après la situation d'urgence

L'ASA doit :

- coordonner le retour dans l'immeuble avec l'ARI;
- avertir le Centre des opérations frontalières (COF) et le Bureau régional de la sécurité ou pour l'Administration centrale, la Section de la sécurité de l'AC, si l'urgence a affecté la zone occupée par l'ASFC;







- veiller à ce que la ligne d'information des employés soit mise à jour en cas de fermeture de l'immeuble.

### 5.10 Section de la sécurité matérielle, Direction de la sécurité et des normes professionnelles (DSNP)

En cas d'urgence, la Section de la sécurité matérielle de la DSNP, fournira une expertise technique aux opérations à l'égard de la protection des biens et des questions de sécurité au cas par cas, en tenant compte que les répercussions peuvent varier selon l'urgence.

## 6. Équipement requis pour les membres de l'Organisme de secours de l'immeuble

Chaque employeur doit acheter l'équipement nécessaire à ses employés qui sont membres de l'Organisme de secours de l'immeuble (OSI).

Tous les membres de l'organisme de secours doivent être clairement et facilement identifiables (casque ou veste colorés, etc.). Des couleurs distinctives doivent être utilisées afin qu'on puisse aisément identifier l'agent de secours en chef, l'adjoint de l'agent de secours en chef, les agents de secours d'étage agents de secours d'étage et les accompagnateurs.

Dans tous les bâtiments, des lampes de poche doivent être fournies à chaque membre de l'OSI et maintenues dans un bon état de fonctionnement.

En raison de leur configuration, les immeubles occupés par 100 personnes ou plus doivent être équipés d'un porte-voix portatif à pile pour faciliter le contrôle d'une foule.







## 7. Équipement de protection contre les incendies et autres

Les propriétaires d'immeubles, les gestionnaires d'immeubles ou TPSGC (immeubles loués) doivent s'assurer que tout l'équipement d'urgence est installé, inspecté et entretenu conformément aux normes et règlements en vigueur.

## 8. Exercices d'évacuation

Un exercice d'évacuation mettant à contribution tous les occupants de l'immeuble doit être organisé au moins une fois l'an. Les exercices partiels peuvent compléter l'exercice d'évacuation complet, mais ils ne devraient pas le remplacer. Un compte rendu de chaque exercice organisé dans l'immeuble doit être conservé pour une période de deux ans à partir de la date de l'exercice.

Il faut communiquer avec le service local des incendies afin d'établir l'horaire et les procédures de notification avant le déclenchement d'un système d'alarme aux fins d'un exercice. Une notification est généralement requise une semaine au moins à l'avance si l'on veut que le service des incendies participe à l'exercice, immédiatement avant le déclenchement d'un système d'alarme-incendie et, par la suite, aussitôt que le système d'alarme-incendie a repris son fonctionnement normal.

Dans les immeubles collectifs où l'ASFC n'est pas le locataire principal, l'agent de secours de l'Agence (ASA) ou le représentant officiel de l'ASFC devrait faire tout son pouvoir pour coordonner un exercice d'évacuation annuel avec les autres occupants de l'immeuble. Si les efforts consentis en ce sens ne sont pas fructueux, l'assistance du Bureau régional de la sécurité ou pour l'Administration centrale, de la Section de la sécurité de l'AC, doit être demandée.

## 9. Plans d'urgence autres que les plans d'évacuation

Les plans d'urgence autres que les plans d'évacuation en cas d'incendie doivent être mis à l'essai au moins tous les deux ans. Les simulations d'exercice sur maquette sont un moyen efficace d'évaluer un plan. Pour se renseigner davantage sur la manière d'effectuer une simulation d'exercice sur maquette, on peut s'adresser à la DSNP.







## 10. Exigences en matière de rapports

Tous les incidents visés par la présente directive doivent être signalés au Bureau régional de la sécurité ou pour l'Administration centrale, à la Section de la sécurité de l'AC, et à la DSNP au moyen d'un rapport d'incident (formulaire BSF152).

Tous incidents reliés aux critères de signalement des évènements doivent être signalés au Centre des opérations frontalières (COF) par téléphone au 613-960-6001, ou par courriel au : CBSA-ASFC_Border Operations Centre-Centre des Opérations Frontalières.

## 11. Formation des membres de l'Organisme de secours de l'immeuble

Chaque membre de l'Organisme de secours de l'immeuble (OSI) doit suivre des séances d'instruction et de formation portant sur les responsabilités qui lui incombent en vertu du plan d'urgence et sur l'utilisation du matériel de protection contre les incendies, au besoin. Les séances de formation devraient comprendre des réunions, des présentations de films ou de bandes vidéo, des exposés par des orateurs invités, des cours de formation et la participation aux activités de la Semaine de prévention des incendies et de la Semaine de la protection civile. Les orateurs invités peuvent provenir du service local des incendies ou de compagnies privées. Les cours d'initiation à l'utilisation des extincteurs ou d'autres appareils sont offerts par les services locaux des incendies ou par des entreprises reconnues qui œuvrent dans les secteurs de la santé et de la sécurité. Pour obtenir des renseignements sur la formation offerte, il faut demander l'assistance du conseiller régional en matière de sécurité et de la Direction de la sécurité et des normes professionnelles (DSNP).

Des documents faisant état de toutes les instructions et de tous les cours de formation donnés aux membres de l'OSI doivent être conservés pour une période de deux (2) ans à compter de la date à laquelle les instructions et la formation ont été fournies.

Tous les membres de l'OSI doivent recevoir une copie du plan d'urgence préparé pour leur immeuble.

L'agent de secours en chef de l'immeuble (ASCI) doit tenir des réunions au moins une fois l'an et après toute modification apportée à la politique, au plan d'évacuation en cas d'urgence ou aux procédures d'urgence relatives à l'immeuble. Durant ces réunions, les membres de l'OSI peuvent se renseigner sur des questions relatives à la planification d'urgence et discuter des sujets qui les préoccupent. Ces réunions sont également l'occasion de mettre à jour les listes des membres de l'OSI et des personnes ayant besoin d'aide.

L'agent de secours en chef de l'immeuble (ASCI) doit conserver un compte rendu de chaque réunion pour une période de deux (2) ans à compter de la date de la réunion. Le compte rendu doit mentionner la date de la réunion, les noms et les titres des personnes présentes et un résumé des questions débattues.







L'agent de secours en chef de l'immeuble (ASCI) doit conserver un compte rendu de chaque exercice pour une période de deux (2) ans à compter de la date de l'exercice. Ce document doit mentionner la date et l'heure de l'exercice et, le cas échéant, la période de temps nécessaire pour évacuer l'immeuble.

## 12. Formation des employés

La direction locale, avec l'aide du comité de santé et de sécurité au travail, doit déterminer la nature et l'étendue des cours d'instruction et de formation requis en milieu de travail. Plus les risques liés au lieu de travail sont importants, plus la formation sera longue et approfondie.

La direction locale doit s'assurer que les instructions que doivent suivre les employés en cas d'urgence, y compris dans une situation d'évacuation, sont affichées dans des endroits bien en vue et que les employés sont au courant des mesures et des procédures à suivre.

Parmi les modes de formation possibles, mentionnons les conférences, les films, les démonstrations pratiques et les brochures d'information.







## 12. Lignes d'information des employés de l'ASFC

La Ligne d'information des employés de l'ASFC, 1-866-NOTICE4 (1-866-668-4234), doit être utilisée par ceux qui souhaitent obtenir des renseignements à jour sur le statut de son lieu de travail en cas de fermeture d'un immeuble. Parmi les situations d'urgence et de perturbation des opérations régulières qui peuvent survenir, mentionnons les intempéries, les catastrophes environnementales, les urgences locales ou nationales, les manifestations et l'occupation des immeubles.

## 13. Programme d'aide aux employés (PAE)

Grâce au programme de gestion du stress provoqué par un incident critique, les employés peuvent discuter des émotions qu'ils ont ressenties et des réactions qu'ils ont eues à la suite d'un accident stressant. Les services d'assistance et de soutien du Programme d'aide aux employés de l'ASFC permettent aux employés de maintenir leur bien-être après avoir vécu un événement traumatisant. À la suite d'un tel événement, le comité de santé et de sécurité au travail dans la région touchée devrait rappeler aux gestionnaires l'importance d'organiser une séance de verbalisation suivant un incident critique à l'intention des employés. Les gestionnaires doivent communiquer avec les Ressources humaines pour obtenir une assistance à cet égard.

## 14. Inspections

Il importe qu'une personne qualifiée (un agent municipal ou un fournisseur de matériel d'urgence techniquement compétent) mène une inspection visuelle de l'immeuble au moins tous les six mois. L'ensemble des escaliers de secours, des sorties de secours, du matériel de protection contre les incendies et d'autres pièces d'équipement de secours de l'immeuble doit être inspecté pour qu'on puisse s'assurer que tout est en bon état de fonctionnement et d'utilisation en tout temps.

Le dossier de chaque inspection doit être daté et signé par la personne qui a mené l'inspection. Il doit être conservé dans l'immeuble inspecté par l'agent de secours en chef de l'immeuble (ASCI) pour une période de deux ans à partir de la date à laquelle il a été signé.

Les membres de l'Organisme de secours de l'immeuble (OSI) doivent signaler toute faille manifeste découverte durant les inspections de routine ou les inspections visuelles quotidiennes aux fonctionnaires compétents afin que ces derniers puissent prendre les mesures correctives nécessaires. Ces anomalies comprennent, entre autres : des portes coupe-feu bloquées en position ouverte ou entre-ouvertes; des sorties, escaliers et corridors obstrués; des lampes d'issues brûlées; du matériel d'intervention hors d'usage ou inaccessible; des risques évidents tels que l'accumulation inutile de matières combustibles; le





mauvais emploi de liquides inflammables; la présence de fils électriques provisoires ou dangereux et d'autres pratiques et conditions non sécuritaires.



# Appendix B: Bomb Threat Procedures – Telephone

## Introduction

Most bomb threats are made by telephone. When you are prepared for such a call, you can respond in a calm manner, ask for specific information about the bomb and listen for some identifying characteristics of the caller. While on the telephone, you may be able to initiate a trace of the telephone number of the caller, providing vital information about the caller's whereabouts.

## 1. Roles and Responsibilities

### 2.1 Duties of employees

Any employees receiving a bomb threat by telephone must:

a) Keep calm;
b) Listen, do not interrupt the caller;
c) Attempt to keep the caller talking and obtain as much information as possible, such as:
- When is the bomb going to explode?
- Where is the bomb located?
- Does the caller realize that people may be killed or injured?
- What does the bomb look like?

d) Note identifying characteristics such as:
- Estimated age;
- Sex;
- Background noises;
- Accent;
- Calm or excited.

e) Refrain from hanging up the phone and initiate call-tracing action if available;
f) Write down everything he or she can remember:
- Record the exact words used by the caller and the time of the call since this information is vital to responders when assessing the credibility of the threat.

g) Do not use walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices;
h) Using a pre-arranged signal to notify your supervisor or a colleague while the call is still ongoing;
i) Notify one of the following people as soon as you can, who will contact the Responsible Building Authority (RBA) immediately:
   - o Supervisor;
   - o Chief Building Emergency Officer;
   - o Deputy Chief Building Emergency Officer;
   - o Floor Emergency Officer and/or Deputy;



- Regional Security Manager or in Headquarters the HQ Security Manager.

j) Avoid discussing the threat with any other employee in order to avoid panic;
k) Remain at your work station until instructed otherwise;
l) Follow the instructions given by the Building Emergency Organization (BEO);
m) If an evacuation is ordered, look around your immediate work area for foreign or suspicious objects and report anything unusual to any member of the BEO;
n) Store classified and protected assets before evacuating **only** if it is safe to do so;
o) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices.

## 2.2 Duties of the Building Emergency Organization (BEO)

Duties of the Responsible Building Authority (RBA)

.

a) Evaluate the circumstances surrounding the threat, assessing the available information and to determine, after discussion with other involved parties, if an evacuation is necessary. To ensure safety of building occupants, evacuation routes must be verified before an evacuation takes place;
b) Direct emergency response;
c) Call Police –**9-1-1** and inform them that a bomb threat has been received;
d) Arrange an escort for the Police Officers on arrival and provide a briefing;
e) Co-ordinate action with other involved parties such as the Chief Building Emergency Officer, the Police and other tenants of the building;
f) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices;
g) Ensure that the Border Operations Center (BOC) is advised by phone at 613-960-6001 or by email at: boc-cof@cbsa-asfc.gc.ca.

Duties of the Chief Building Emergency Officer (CBEO)

a) Alert the Floor Emergency Officers by telephone or other method;
b) Advise the Workplace Health and Safety Committee;
c) Contact the Deputy Building Emergency Officer;
d) Alert other building occupants;
e) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices.

Duties of the Floor Emergency Officer(s) and Deputies

a) Instruct employees to conduct a cursory check of their own workspace for suspicious packages;
b) If a suspicious package is found:
    - instruct employees to avoid touching it;







- instruct employees to evacuate the immediate area; and,
- advise the RBA (Refer to **Appendix C**: "Suspicious Packages Procedures").

c) Advise employees to take personal belongings with them;
d) Await instructions from the RBA before evacuating the building;
e) Evacuate the building as per fire evacuation procedures when instructed by the RBA;
f) Make sure employees are at least 100m away from the building;
g) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices.

### 2.3 Verification of Evacuation Routes

a) If the decision to evacuate is taken by the Responsible Building Authority, a cursory check of evacuation routes and public areas must be done to preclude the possibility of an evacuation being impeded;
b) When instructed by the RBA, members of the BEO will check evacuation routes and public areas which may include, depending on building layout, the following:
    a. Corridors and washrooms;
    b. Stairwells (where applicable);
    c. Lobby;
    d. Emergency exits.
c) Immediately advise the Deputy Chief Building Emergency Officer of areas checked;
d) If a suspicious object is found, it must not be touched, the immediate area must be evacuated and the Chief Building Emergency Officer must be notified of the location of the object. The nature of the object must be confirmed and its removal must be left to the police;
e) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating device.



# Annexe B : Procédure en cas d'alerte à la bombe – Téléphone

## 1. Introduction

La plupart des alertes à la bombe se font par téléphone. Si vous êtes préparé à recevoir un tel appel, vous pouvez intervenir calmement, demander des renseignements précis concernant la bombe et porter attention à des détails permettant d'identifier l'appelant. Pendant que l'appelant est au téléphone, vous pourrez peut-être faire dépister son numéro de téléphone, ce qui fournirait des renseignements importants concernant le lieu où il se trouve.

## 2. Rôles et responsabilités

### 2.1 Obligations des employés

Tout employé qui reçoit une alerte à la bombe doit :

a) rester calme;
b) écouter et ne pas interrompre son interlocuteur;
c) tenter de faire parler l'appelant le plus longtemps possible afin d'obtenir le plus de renseignements possible, entre autres :
   - à quel moment la bombe explosera-t-elle?
   - où est placé l'engin?
   - se rend-il compte que des personnes peuvent être tuées ou blessées?
   - quelle est l'apparence de l'engin?
d) relever des caractéristiques pouvant identifier l'appeler, notamment :
   - son âge approximatif;
   - son sexe;
   - les bruits de fond;
   - son accent;
   - le ton (calme ou agité);
e) s'abstenir de raccrocher le téléphone et prendre des mesures de dépistage d'appels si possible;
f) écrire tout ce que l'appelant dit :
   - transcrire les mots exacts prononcés par l'appelant ainsi que l'heure de l'appel du fait que cette information est essentielle aux intervenants qui doivent évaluer la crédibilité de la menace;
g) ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe;
h) aviser son superviseur au moyen d'un signal convenu d'avance pendant que l'appelant est au téléphone;



i) informer dès que possible l'une des personnes suivantes, qui communiquera immédiatement avec l'autorité responsable de l'immeuble (ARI) :
   - superviseur;
   - agent de secours en chef de l'immeuble;
   - adjoint de l'agent de secours en chef de l'immeuble;
   - agent de secours d'étage ou son adjoint;
   - gestionnaire régional de la sécurité ou pour l'Administration centrale, le gestionnaire de la sécurité de l'AC;

j) éviter de parler de la menace avec un autre employé afin d'éviter la panique;
k) demeurer à son poste de travail jusqu'à avis contraire;
l) observer les consignes transmises par l'Organisme de secours de l'immeuble;
m) si une évacuation est ordonnée, examiner la zone de travail immédiate pour vérifier la présence d'objets étrangers ou suspects et signaler toute observation inhabituelle à un membre de l'OSI;
n) entreposer les biens classifiés et protégés avant d'évacuer **uniquement** s'il est sécuritaire de le faire;
o) ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe.

## 2.2 Fonctions de l'Organisme de secours de l'immeuble (OSI)

Fonctions de l'autorité responsable de l'immeuble (ARI)

a) Évaluer les circonstances entourant la menace, évaluer l'information disponible et déterminer si l'évacuation est nécessaire après avoir discuté de cette possibilité avec les autres parties. Pour garantir la sécurité des occupants, les chemins d'évacuation doivent être vérifiés avant d'être utilisés;
b) Diriger les interventions d'urgence;
c) Appeler la police au **9-1-1** et l'aviser qu'une alerte à la bombe a été reçue;
d) Affecter une escorte pour accueillir les policiers à leur arrivée et les mettre au courant de la situation;
e) Coordonner l'intervention avec d'autres parties concernées telles que l'agent de secours en chef de l'immeuble, les services de police et les autres locataires de l'immeuble;
f) Ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe;
g) S'assurer d'informer le Centre national des opérations frontalières par téléphone au 613-960-6001 ou par courriel à : boc-cof@cbsa-asfc.gc.ca.



Fonctions de l'agent de secours en chef de l'immeuble (ACSI)

a) Alerter les agents de secours d'étage par téléphone ou autre moyen;
b) Aviser le comité de santé et de sécurité au travail;
c) Communiquer avec l'adjoint de l'agent de secours de l'immeuble;
d) Alerter les autres occupants de l'immeuble;
e) Ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe.

Fonctions des agents de secours en chef d'étage et de leurs adjoints

a) Demander aux employés de chercher tout colis suspect dans leur espace de travail;
b) Si un colis suspect est repéré :
   - ordonner aux employés de ne pas toucher au colis;
   - ordonner aux employés d'évacuer la zone immédiate;
   - conseiller l'ARI (voir l'**annexe C** : « Procédures à suivre en cas de colis suspects »).
c) Aviser les employés d'apporter leurs effets personnels;
d) Attendre les instructions de l'ARI avant d'évacuer les lieux;
e) Évacuer l'immeuble en suivant les procédures d'évacuation en cas d'incendie lorsque l'ARI donne des instructions en ce sens;
f) S'assurer que les employés s'éloignent à au moins 100 mètres de l'immeuble;
g) Ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe.

**2.3 Vérification des chemins d'évacuation**

a) Si l'autorité responsable de l'immeuble décide de faire évacuer l'immeuble, il faut faire une vérification superficielle des chemins d'évacuation et des aires publiques afin d'éviter que l'évacuation ne soit entravée;
b) Lorsque l'ARI donne une instruction en ce sens, les membres prédésignés de l'OSI vérifieront les chemins d'évacuation et les aires publiques, qui peuvent inclure les lieux suivants, selon le schéma d'aménagement du bâtiment :
   a. couloirs et salles de bain;
   b. puits d'escalier (s'il y a lieu);
   c. entrée;
   d. issues de secours.
c) Indiquer immédiatement à l'adjoint de l'agent de secours en chef de l'immeuble les aires qui ont été vérifiées;
d) Si un objet suspect est découvert, il fait éviter d'y toucher, faire évacuer les environs immédiats et informer l'agent de secours en chef de l'immeuble du lieu où se trouve







l'objet. La nature de l'objet doit être confirmée, et il faut laisser aux services de police la tâche de retirer l'objet des lieux;

e) Ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe.





# Appendix C: Suspicious Packages Procedures

## 1. Introduction

A **"suspicious package"** is defined as a letter, package, parcel, bag, canister, box, etc., which raises suspicion that there may be a maliciously placed **biological, chemical, radiological or explosive** hazard within.

Suspicious packages could be delivered to the workplace, so it is good practice to be vigilant and aware of what to do. Employees know what kind of mail and packages they usually receive. They should note things that are out of the ordinary, such as unexpected mail from a foreign country. Certain indicators can raise suspicions that a suspicious package is present, such as:

a) Excessive postage;
b) Handwritten or poorly typed addresses;
c) Incorrect titles;
d) Title, but no name;
e) Misspellings of common words;
f) Oily stains, discolorations or odour;
g) No return address;
h) Excessive weight;
i) Lopsided or uneven envelope;
j) Protruding wires or aluminum foil;
k) Excessive security material such as masking tape, string, etc.;
l) Visual distractions;
m) Marked with restrictive endorsements, such as "Personal" or "Confidential" or "Do not X-ray"; or
n) Shows a city or province/state in the postmark that does not match the return address.

The contents of a letter or package may cause concern if:

a) Powder or a liquid is visible;
b) It contains a threatening note;
c) It contains an object that is not expected to be received or cannot be identified.

## 2. Roles and Responsibilities

### 2.1 Duties of employees

Anyone who receives a suspicious package will:

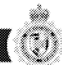


a) Stay calm;
b) Reduce further contact with the package (do not handle, shake, smell or taste it);
c) Leave the package where it is. If it is unopened, do not open it;
d) Ensure that all individuals evacuate the room and close the door;
e) Isolate the hazard by minimizing **time** exposed, taking safe/reasonable **distance** (at least 25 meters) from the hazard, and using any physical **shielding** available;
f) Note identifying characteristics such as:
    - What does it look like – size, materials?
    - Where is it located?
    - How big is the package?
    - Is there any noise coming from the package?
    - Is anything written on the package?
    - Any oils, stains, or discolouration?
g) Move, along with any other possibly affected employees, to a designated, safe and isolated location. This will avoid cross contamination and facilitate response by health officials, decontamination, medical assessment, treatment, etc.;
h) Note the time of incident, names of people within the area of concern and other relevant details;
i) Notify one of the following people as soon as you can, who will contact the Responsible Building Authority (RBA) immediately:
    - Immediate supervisor;
    - Chief Building Emergency Officer;
    - Deputy Chief Building Emergency Officer;
    - Floor Emergency Officer and/or Deputy;
    - Regional Security Manager or in Headquarters the HQ Security Manager.
j) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices;
k) Wait for instructions from responding health officials or emergency authorities.
l) If possible, while in the secure area, wash hands with soap and water;
m) Keep hands away from eyes, mouth and ears to reduce possible contamination;
n) It is crucial to avoid cross contamination of other people. Staying in a secure area with other exposed persons will facilitate response by emergency crews.

All employees must be informed of the expected response to emergency situations. It is important to note that there are existing treatments (either decontamination or antibiotics) for dangerous agents, including anthrax.

## 2.2 Duties of the Building Emergency Organization (BEO)

Duties of the Responsible Building Authority (RBA)



The Responsible Building Authority is responsible for assessing the threat and recommending, after discussion with other involved parties, the evacuation of the building. If no one can identify the package, the RBA must:

a) Direct emergency response;
b) Ensure package is isolated;
c) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices;
d) Co-ordinate action with other involved parties:—
    - Chief Building Emergency Officer;
    - Police (911 or other local emergency number) - Contact authorities and inform them that a package of concern/ suspicious package has been found and that emergency procedures are in progress. Arrange an escort for Fire Department, Health Officials and Police Officers on arrival and provide a briefing; follow instructions from these responding agencies and advise the Chief Building Emergency Officer accordingly;
    - Property manager/owner;
    - Other tenants of the building;
    - Regional Security Manager or in Headquarters the HQ Security Manager.
e) Ensure that personnel who may have been exposed are assembled in one safe area. Avoiding possible cross contamination is crucial;
f) Cooperate with responding agencies. If the responding agencies advise that a building evacuation is necessary, instruct the Chief Building Emergency Officer accordingly;
g) Ensure that the Border Operations Center (BOC) is advised by phone at 613-960-6001 or by email at: boc-cof@cbsa-asfc.gc.ca.

Duties of the Chief Building Emergency Officer

a) Evacuate immediate area;
b) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices;
c) Arrange for the shutdown of Heating, Ventilation, and Air Conditioning Systems (HVAC);
d) Follow instructions from the Responsible Building Authority;
e) Alert the Floor Emergency Officers by telephone or other method;
f) Advise the Occupational Health and Safety Committee.

Duties of the Deputy (and Deputy Alternate) Chief Building Emergency Officer

a) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices;
b) If instructed by the RBA, evacuate the building according to appropriate evacuation procedures, i.e., as per fire evacuation procedures.










Duties of the Floor Emergency Officer(s) and Deputies

a) Refrain from using walkie-talkies, two-way radios, or cell phones for communicating as these could trigger detonating devices;
b) Await instructions from the Chief Building Emergency Officer;
c) If instructed by the Chief Building Emergency Officer, evacuate the building according to appropriate evacuation procedures, i.e., as per fire evacuation procedures;
d) Make sure employees are assembled in a safe area at least 100m away from the building if an evacuation takes place.







# Annexe C : Procédures à suivre en cas de colis suspects

## 1. Introduction

Un « colis suspect » est une lettre, un colis, un paquet, un sac, une boîte, un contenant, etc., qui peut porter à croire qu'il contient à des fins malveillantes un produit **biologique, chimique, radiologique ou explosif** dangereux.

Des colis suspects pourraient être livrés sur le lieu de travail. Il est donc conseillé de faire preuve de vigilance et de savoir de ce qu'il convient de faire. Les employés connaissent le type d'enveloppes et de colis qu'ils reçoivent normalement. Ils doivent remarquer les détails qui sortent de l'ordinaire, par exemple, du courrier inattendu en provenance d'un pays étranger. Certains indicateurs peuvent permettre de soupçonner qu'il s'agit d'un colis suspect :

a) affranchissement excessif;
b) adresse écrite à la main ou mal dactylographiée;
c) titres inexacts;
d) titre sans nom;
e) fautes d'orthographe dans des mots communs;
f) taches d'huile, décoloration ou odeur;
g) absence d'une adresse de l'expéditeur;
h) poids excessif;
i) enveloppe inégale;
j) fils ou papier d'aluminium faisant saillie;
k) emballage excessif, comme du ruban gommé ou une cordelette;
l) distractions visuelles;
m) mentions restrictives, comme « Personnel », « Confidentiel » ou « Ne pas radiographier »;
n) mention d'une ville, d'une province ou d'un État dans le cachet de la poste qui ne correspond pas à l'adresse de l'expéditeur.

Le contenu d'une lettre ou d'un colis peut être une source d'inquiétude si :

a) de la poudre ou un liquide est visible;
b) le colis contient une lettre de menace;
c) le colis contient un objet dont on n'attendait pas la venue ou qui ne peut être identifié.

## 2. Rôles et responsabilités

### 2.1 Obligations des employés





Quiconque reçoit un colis suspect doit :

a) demeurer calme;
b) éviter le plus possible tout nouveau contact avec le colis (ne pas le manipuler, l'agiter, le sentir ou le goûter);
c) laisser le colis là où il se trouve, et s'il n'est pas ouvert, ne pas l'ouvrir;
d) s'assurer que tous les gens évacuent la pièce et fermer la porte;
e) isoler le risque en diminuant le plus possible le **temps** d'exposition, s'éloigner à une **distance** raisonnable/sûre (au moins 25 mètres) et utiliser tout **bouclier** physique disponible;
f) relever des caractéristiques pouvant l'identifier, notamment :
   - quelle est l'apparence du colis – dimension, matériau?
   - où se trouve-t-il?
   - quelle est sa taille?
   - des bruits émanent-ils du colis?
   - quelles sont les mentions sur le colis?
   - y a-t-il des traces d'huile, des taches ou de la décoloration?
g) se rendre en compagnie des autres employés du secteur à un endroit désigné, sûr et isolé, ce qui évitera la contamination croisée et facilitera l'intervention des représentants de la santé, la décontamination, l'évaluation médicale, les traitements, etc.;
h) noter l'heure de l'incident, les noms de personnes qui se trouvaient dans le secteur concerné et tout autre détail pertinent;
i) informer dès que possible l'une des personnes suivantes, qui communiquera immédiatement avec l'autorité responsable de l'immeuble (ARI) :
   - superviseur immédiat;
   - agent de secours en chef de l'immeuble;
   - chef adjoint de secours de l'immeuble;
   - agent principal ou adjoint de secours d'étage;
   - gestionnaire régional de la sécurité ou pour l'Administration centrale, le gestionnaire de la sécurité de l'AC.
j) ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe;
k) attendre les instructions des autorités sanitaires ou des services d'urgence;
l) s'il y a lieu, se laver les mains avec du savon et de l'eau dans l'aire protégée;
m) ne pas se toucher les yeux, la bouche et les oreilles pour éviter toute contamination;
n) du fait qu'il faut éviter à tout prix la contamination croisée, demeurer dans l'aire protégée avec les autres personnes qui ont été exposées afin de faciliter la tâche des équipes d'urgence.



Les employés doivent connaître la réaction attendue face à une urgence. Il faut se rappeler que des traitements existent (décontamination et antibiotiques) contre des agents dangereux, dont l'anthrax.

**2.2 Fonctions de l'organisme de secours de l'immeuble (OSI)**

Fonctions de l'autorité responsable de l'immeuble (ARI)

L'autorité responsable de l'immeuble est chargée d'évaluer la menace et de recommander l'évacuation de l'immeuble après avoir discuté de cette éventualité avec les autres parties en cause. Si personne ne peut identifier le colis, l'ARI doit :

a) diriger l'intervention d'urgence;
b) s'assurer que le colis est isolé;
c) ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe;
d) coordonner les mesures avec les autres parties en cause :
    - agent de secours en chef de l'immeuble;
    - services policiers (911 ou autre numéro d'urgence local) – appeler les autorités et les aviser qu'un colis préoccupant/suspect a été découvert et que les mesures d'urgence sont en cours; affecter une escorte pour accompagner les membres du service d'incendie, les représentants de la santé et les policiers à leur arrivée et les mettre au courant de la situation; suivre les instructions de ces intervenants et aviser l'agent en chef de secours de l'immeuble en conséquence;
    - gestionnaire/propriétaire de l'immeuble;
    - autres locataires de l'immeuble;
    - gestionnaire régional de la sécurité ou pour l'Administration centrale, le gestionnaire de la sécurité de l'AC;
e) veiller à ce que les personnes qui ont pu être exposées soient regroupées dans un endroit sûr du fait qu'il faut à tout prix éviter la contamination croisée;
f) collaborer avec les intervenants; si ceux-ci déclarent que l'immeuble doit être évacué, aviser l'agent de secours en chef de l'immeuble en conséquence;
g) S'assurer d'informer le Centre national des opérations frontalières par téléphone au 613-960-6001 ou par courriel à : boc-cof@cbsa-asfc.gc.ca.

Fonctions de l'agent de secours en chef de l'immeuble

a) Évacuer le secteur immédiat;







b) Ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe;
c) Faire éteindre le système de chauffage, de ventilation et de climatisation;

d) Suivre les instructions de l'autorité responsable de l'immeuble;
e) Alerter les agents de secours d'étage par téléphone ou autre moyen;
f) Aviser le comité de santé et de sécurité au travail.

Fonctions du chef adjoint de secours de l'immeuble et de son suppléant

a) Ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe;
b) Si l'autorité responsable de l'immeuble donne des instructions en ce sens, évacuer l'immeuble en suivant les procédures d'évacuation en cas d'incendie.

Fonctions des agents principaux et adjoints de secours d'étage

a) Ne pas utiliser d'émetteurs-récepteurs portatifs, d'appareils radios bidirectionnels ou de téléphones cellulaires pour communiquer, car ces appareils pourraient déclencher une bombe;
b) Attendre les directives de l'Agent de secours en chef de l'immeuble;
c) Si l'Agent de secours en chef de l'immeuble donne des instructions en ce sens, évacuer l'immeuble en suivant les procédures d'évacuation en cas d'incendie;
d) En cas d'évacuation, s'assurer que les employés se rassemblent à une distance sûre d'au moins 100 mètres de l'immeuble.



# Appendix D: Hostage Taking Emergency Plan - Procedures

This procedure applies to all non-operational CBSA office space and should be read in conjunction with the:

- Emergency and Essential Information page on Atlas under the "Health, Safety and Security" main menu tab;
- Guideline in the Event of a Critical Injury or Death of an Employee in the Line of Duty, and;
- Critical Incident Stress Management (CISM) Guidelines and Standard Operating Procedures.

In the case of armed CBSA officers trained in the use of force, the responses dictated by their training, the procedure in the Arming Policy Suite, and the applicable Regional Critical Incident Management Plan, developed in accordance with the Emergency Preparedness, All Hazards Approach will take precedence.

## Introduction

A hostage taking is a situation in which a person or persons hold another person or persons against their will by force, threat, or violence. Although a hostage situation is unlikely, the possibility cannot be discounted and the impact to the individual is high.

The Hostage Taking Emergency Plan should be prepared based on recommendations from the local Police Department.

## 1. Roles and Responsibilities

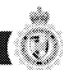
### 2.1 Duties of employees

If you see/hear/witness a hostage situation taking place:

a) Do not intervene;
b) Get away from being in immediate danger;
c) Call 911;
d) Provide as much information as possible; i.e., location of incident; number of hostage takers and hostages; physical description and names of the hostage takers (if known);







any weapons the hostage takers may have; and your name, location and phone number;

e) Notify one of the following people as soon as you can, who will contact the Responsible Building Authority (RBA) immediately:
   - Supervisor;
   - Chief Building Emergency Officer;
   - Deputy Chief Building Emergency Officer;
   - Floor Emergency Officer and/or Deputy;
   - Regional Security Manager or in Headquarters the HQ Security Manager.

If you are taken hostage:

a) Remain calm, be polite, and cooperate;
b) Speak only when spoken to;
c) Do not try to be a negotiator;
d) Do not volunteer suggestions or courses of action;
e) Do not attempt to escape unless there is an extremely good chance for survival. It is better to be submissive and obey your captor(s);
f) Speak normally. Do not complain or become belligerent. Comply with all orders and instructions;
g) Avoid getting into political or ideological discussions with your captor(s);
h) If there is more than one hostage taker, do not take sides, do not appear to favor one more than the other;
i) Do not draw attention to yourself with sudden body movements, comments or hostile looks;
j) Stay as far away from the hostage taker(s) as possible, preferably in a corner out of the way;
k) Be aware that help is being organized;
l) Carefully observe the captor(s) and try to memorize their physical traits, voice patterns, clothing, and other details that can help provide a description later.

### 2.2 Duties of the Building Emergency Organization (BEO)

Duties of the Responsible Building Authority (RBA)

a) Ensure that police have been notified via "911" and the situation reported;
b) Evacuate the immediate area and close access;

c) Inform the Regional Security Office who in turn will contact the Security and Professional Standards Directorate (SPSD) at Headquarters;
d) Arrange an escort for the Police Officers on arrival and provide a briefing;
e) Co-ordinate action with other involved parties such as the Chief Building Emergency Officer, the Police and other tenants of the building;
f) Ensure that the Border Operations Center (BOC) is advised by phone at 613-960-6001 or by email at: boc-cof@cbsa-asfc.gc.ca.

Duties of the Chief Building Emergency Officer, Floor Emergency Officer(s) and Deputies

a) Assist the BEO as required.



# Annexe D: Plan d'urgence – Prise d'otages

La présente procédure s'applique à tous les bureaux de l'ASFC non opérationnel et doit être lue en parallèle avec ce qui suit :

- la page Renseignements essentiels et d'urgence dans Atlas, sous l'onglet « Santé et sécurité » du menu principal;
- Lignes directrices en cas de blessures graves ou de mort d'un employé dans l'exercice de ses fonctions; et
- Lignes directrices et procédures normales en cas de gestion du stress dû à un incident critique (GSIC).

Dans le cas des agents armés de l'ASFC ayant reçu une formation sur le recours à la force, les interventions dictées par leur formation, la procédure de la Suite de la politique d'armement et le plan régional de gestion des incidents critiques qui s'applique, élaboré en conformité avec le document Mesures d'urgence, une approche globale auront préséance.

## 1. Introduction

Une prise d'otage est une situation dans laquelle une ou plusieurs personnes détiennent une autre ou d'autres personnes contre leur gré par la force, la menace ou la violence. Bien qu'une prise d'otages demeure peu probable, la possibilité qu'une telle situation se produise ne peut être ignorée et ses répercussions pour la personne prise en otage sont élevées.

Le plan d'intervention d'urgence en cas de prise d'otages doit être élaboré en fonction des recommandations du service de police local.

## 2. Rôles et responsabilités

### 2.1 Obligations des employés

Pour les employés qui sont témoins d'une prise d'otage

a) Ne pas intervenir.
b) S'éloigner du danger immédiat.
c) Appeler le 911.



d) Fournir le plus de renseignements possible, c'est-à-dire le lieu de l'incident, le nombre de preneurs d'otages et d'otages, la description physique et les noms des preneurs d'otages (si ces détails sont connus), les armes que les preneurs d'otages pourraient avoir en leur possession ainsi que le nom de l'appelant, le lieu où il se trouve et son numéro de téléphone.
e) Informer dès que possible l'une des personnes suivantes, qui communiquera immédiatement avec l'autorité responsable de l'immeuble (ARI) :
   - superviseur;
   - agent de secours en chef de l'immeuble;
   - adjoint de l'agent de secours en chef de l'immeuble;
   - agent de secours d'étage ou son adjoint;
   - gestionnaire régional de la sécurité ou pour l'Administration centrale, le gestionnaire de la sécurité de l'AC.

Pour les employés pris en otage

a) Rester calme, être poli et coopérer.
b) Parler seulement si le ou les preneurs d'otages adressent la parole à l'employé.
c) Ne pas essayer de négocier.
d) Ne pas faire de suggestions ou proposer une marche à suivre.
e) Ne pas tenter de s'échapper à moins d'avoir une extrêmement bonne chance de survie. Il vaut mieux se soumettre et obéir aux ordres du ou des preneurs d'otages.
f) Parler normalement. Ne pas se plaindre ou devenir agressif. Se conformer à tous les ordres et à toutes les instructions.
g) Éviter d'entrer dans des discussions politiques ou idéologiques avec le ou les preneurs d'otages.
h) S'il y a plusieurs preneurs d'otages, rester neutre et ne pas montrer de favoritisme pour l'un plus que l'autre.
i) Ne pas attirer l'attention sur soi par des mouvements brusques, des commentaires ou des regards hostiles.
j) S'éloigner le plus possible du ou des preneurs d'otages, de préférence dans un coin.
k) Se rappeler que les autorités organisent une intervention de secours.
l) Observer soigneusement le ou les preneurs d'otages et essayer de mémoriser leurs traits physiques, leurs empreintes vocales, leurs vêtements et d'autres détails qui pourraient aider à fournir une description plus tard.



## 2.2 Fonctions de l'Organisme de secours de l'immeuble (OSI)

Fonctions de l'autorité responsable de l'immeuble (ARI)

a) S'assurer que quelqu'un a appelé les policiers en composant le 911 et que la situation a été signalée.
b) Évacuer le secteur immédiat et bloquer l'accès.
c) Informer le Bureau régional de sécurité qui, à son tour, communiquera avec la Direction de la sécurité et des normes professionnelles (DSNP) à l'Administration centrale.
d) Affecter une escorte pour accueillir les policiers à leur arrivée et les mettre au courant de la situation.
e) Coordonner l'intervention avec d'autres parties concernées telles que l'agent de secours en chef de l'immeuble, les services de police et les autres locataires de l'immeuble.
f) S'assurer d'informer le Centre national des opérations frontalières par téléphone au 613-960-6001 ou par courriel à : boc-cof@cbsa-asfc.gc.ca.

Fonctions de l'agent de secours en chef de l'immeuble, des agents de secours d'étage et de leurs adjoints

a) Aider l'OSI au besoin.







# Appendix E: Earthquakes Procedures

## 1. Introduction

Some of our offices are located in an earthquake zone. Depending on the magnitude of the earthquake, the emergency is handled by the municipality and then the province. If the earthquake is beyond what can be handled by the municipality and the province, the province will request aid from Public Safety Canada who will coordinate the federal response.

People may not be forewarned; the shock or tremor may provide the only warnings.

## 2. Roles and Responsibilities

### 2.1 Duties of employees

a) Do not run outdoors;
b) Remain calm;
c) Take immediate shelter under tables, desks, or other such object that will offer protection against flying glass or debris, and protect your head and neck;
d) If possible, keep at least 5 meters away from windows to avoid flying glass. Keep away from skylights and large overhead light fixtures;
e) Step under a doorway or strong structural column if no desk, table, etc. is available;
f) If fire occurs, operate the nearest manual fire alarm, evacuate and notify the local Fire Department;
g) After the major tremor, evacuate the building only when instructed by the Floor Emergency Officers and deputies, as it may be safer to remain in the building. **REMEMBER aftershocks or additional tremors may occur**;
h) When evacuating the building be careful of falling glass, brick, electric wires, or other hazardous objects;
i) Employees should meet at the pre-determined meeting place;
j) Stay away from waterfront areas. Large earthquakes at sea are often followed by tidal waves;
k) Do not re-enter the building until told so by the building authority, as they must check for any structural damage;
l) Render first aid and rescue as necessary. Call for an ambulance, if required.
m) Reserve telephones for emergency calls only;
n) Call the Employee Notice Line (1-866-668-4234) to receive a status update on when you should return to work, if you have been sent home.



## 2.2 Duties of the Building Emergency Organization (BEO)

Duties of the Responsible Building Authority

After the tremor:

a) Contact the members of the Building Emergency Organization and ask for a status report;

b) Order immediate evacuation if there is fire, major structural damage or leaking gas;

c) Contact the Municipal Fire Department for advice on the decision to evacuate or not;
d) Direct the emergency response;
e) Ensure that the Border Operations Center (BOC) is advised by phone at or by email at: boc-cof@cbsa-asfc.gc.ca.

Duties of the Chief Building Emergency Officer

After the tremor:

a) Contact the building maintenance supervisor to make sure utilities, gas, electricity and water are turned off. The building maintenance supervisor will also be responsible for checking water and sewage lines. The fire alarms and the sprinkler system may activate as a result of the earthquake;
b) Contact the Occupational Health and Safety Committee;
c) Contact the Deputy Building Emergency Officer and ask to check out the evacuation routes for obstructions;
d) Contact the Floor Emergency Officers and advise them what actions to take;
e) Listen to your local radio station on your battery-operated radio for emergency instructions from the municipality or province.

Duties of the Floor Emergency Officers

After the tremor:

a) Immediately assess the damage and casualties and advise the Chief Building Emergency Officer;
b) Keep employees calm and administer first aid as required;
c) Evacuate immediately if there is fire, major structural damage or a gas leak;
d) If there is no immediate danger ask employees to remain calm until instructions are received from the Chief Building Emergency Officer. It may be safer to remain in the building;





e) Evacuate your area when instructed by the Chief Building Emergency Officer and advise the chief when the floor has been cleared or any problems encountered.



# Annexe E : Procédures en cas de séisme

## 1. Introduction

Certains de nos bureaux sont situés dans une zone sismique. Selon la magnitude du séisme, les mesures d'urgence sont prises par la municipalité, puis par la province. Si les mesures requises par le séisme excèdent la capacité de l'administration municipale et de la province, celle-ci demandera l'aide de Sécurité publique Canada (SPC), qui coordonnera l'intervention fédérale.

La population peut ne pas être prévenue, et les secousses peuvent constituer le seul avertissement.

## 2. Rôles et responsabilités

### 2.1 Obligations des employés

a) Ne pas se rendre à la hâte à l'extérieur ;
b) Rester calme ;
c) Se réfugier immédiatement sous une table, un bureau ou tout autre objet qui offre une protection contre les éclats de verre ou les débris, et protéger sa tête et son cou ;
d) Se tenir à au moins cinq mètres des fenêtres pour se protéger contre les éclats de verre. S'éloigner des lanterneaux et des gros plafonniers ;
e) Se tenir sous un cadre de porte ou une solide poutre structurale si aucun bureau, aucune table, etc., n'est disponible;
f) Si un incendie éclate, actionner l'avertisseur d'incendie à commande manuelle le plus proche, évacuer les lieux et alerter le service local des incendies ;
g) Après le choc principal, n'évacuer le bâtiment que si les agents de secours d'étage et leurs adjoints en donnent l'ordre étant donné qu'il est possible que les employés soient plus en sécurité à l'intérieur de l'immeuble. **NE PAS OUBLIER que des répliques ou d'autres secousses peuvent survenir ;**
h) Au moment d'évacuer l'immeuble, porter attention aux éclats de verre, aux briques, aux fils électriques et aux autres objets dangereux qui tombent ;
i) Les employés doivent tous se rendre au lieu de rassemblement convenu ;
j) Rester loin des zones riveraines. Les séismes de grande magnitude qui se produisent dans les fonds marins sont souvent suivis par des raz-de-marée ;



k) Ne pas retourner dans l'immeuble avant d'en avoir reçu l'autorisation par l'autorité responsable de l'immeuble du fait que la présence d'éventuels dommages structurels doit être vérifiée;
l) Au besoin, fournir des services de premiers soins et de sauvetage. Appeler les services ambulanciers, si nécessaire ;
m) N'utiliser les téléphones que pour les appels d'urgence ;
n) Appeler la ligne d'information des employés (1-866-668-4234) pour savoir quand l'autorisation de retourner au travail sera donnée, pour les employés qui ont été renvoyés à la maison.

### 2.2 Fonctions de l'Organisme de secours de l'immeuble (OSI)

Fonctions de l'autorité responsable de l'immeuble

Après le séisme :

a) Communiquer avec l'Organisme de secours de l'immeuble et demander un rapport de la situation ;

b) Évacuer immédiatement l'immeuble en cas d'incendie, de dommages structuraux importants ou de fuite de gaz ;

c) Communiquer avec le service d'incendie municipal pour obtenir des conseils sur la décision d'évacuer ou non l'immeuble;

d) Diriger l'intervention d'urgence ;
e) S'assurer d'informer le Centre national des opérations frontalières par téléphone au ou par courriel à : boc-cof@cbsa-asfc.gc.ca.

Fonctions de l'agent de secours en chef de l'immeuble

Après le séisme :
a) Communiquer avec le superviseur de l'entretien de l'immeuble pour s'assurer que l'alimentation en gaz, en électricité et en eau a été coupée. Le superviseur vérifiera également les conduites d'eau et d'égout. Le séisme peut activer les alarmes d'incendie et les gicleurs ;
b) Communiquer avec le comité de santé et de sécurité au travail ;







c) Communiquer avec l'adjoint de l'agent de secours de l'immeuble et demander que l'équipe de secours vérifie si les voies d'évacuation sont accessibles ;
d) Communiquer avec les agents de secours d'étage et les informer des mesures à prendre ;
e) Rester à l'écoute des nouvelles locales sur le poste radio à piles pour prendre connaissance des instructions d'urgence de la municipalité ou de la province.

Fonctions de l'agent de secours d'étage

Après le séisme :

a) Immédiatement après la secousse, évaluer les dégâts et les victimes et alerter l'agent de secours en chef de l'immeuble ;
b) Demander aux employés de rester calmes et apporter au besoin les premiers soins ;
c) Évacuer l'immeuble en cas d'incendie, de dommages structuraux importants ou de fuite de gaz ;
d) S'il n'y a aucun danger immédiat, demander aux employés de rester calmes en attendant que des instructions soient reçues de l'agent de secours en chef de l'immeuble. Il peut être plus sécuritaire de rester dans l'immeuble ;
e) Évacuer le secteur si l'agent de secours en chef de l'immeuble le demande. Communiquer par la suite avec l'agent de secours en chef lorsque l'étage aura été évacué ou si des problèmes sont constatés.







# Appendix F: Flood Emergency Procedures

## 1. Introduction

Floods are the most frequent natural hazard in Canada. They can occur at any time of the year and are most often caused by heavy rainfall, rapid melting of a thick snow pack, ice jams, or more rarely, the failure of a natural or man-made dam.

Spring flooding is most prevalent in the Prairies, the Atlantic and Quebec Regions due to an overflow of the river systems.

## 2. Definition

**Flash flood**: a sudden, localized flood of great volume of water over dry land, typically caused by unusually heavy rain which can reach its peak volume in a matter of a few minutes.

## 3. Roles and Responsibilities

### 2.1 Duties of the Building Emergency Organization (BEO)

Duties of the Responsible Building Authority (RBA)

Before a flood:

a) Find out if the facility is located in a flood plain by contacting the Regional Security Officer as well as local authorities;

b) Learn about the community's emergency plans, warning signals, evacuation routes, and locations of emergency shelters;

c) Develop flood procedures to protect individuals and equipment and add them to the Building Emergency Response Plan.

During a flood:

a) Contact the Municipal Fire Department or local authorities for advice on whether or not to evacuate;
b) Direct the emergency response for the building;





c) Ensure that the Border Operations Center (BOC) is advised by phone at or by email at: boc-cof@cbsa-asfc.gc.ca.

Duties of the Chief Building Emergency Officer (CBEO)

During a flood warning:

a) Monitor the electronic media for information about rising water levels and advise the RBA;
b) Review the flood procedures with the Building Emergency Organization members and key employees;

During a flood:

c) If it appears that an evacuation might be necessary, contact the building maintenance supervisor to make sure utilities, gas, electricity and water are turned off;
d) If applicable, have the elevators raised to the second floor and turn off power;
e) If ordered by the RBA, lead the building evacuation according to appropriate evacuation procedure.

Duties of the Floor Emergency Officer(s) and Deputies

During a flood warning:

a) Review the flood procedures with the Building Emergency Organization members and key employees;
b) Await instructions from the CBEO;
c) If instructed by the CBEO, evacuate the building according to appropriate evacuation procedures;
d) Ensure employees safety during the building evacuation.

### 2.2 Duties of employees

During a flood:

a) Stay calm;
b) Remain in existing location unless instructed otherwise by the members of the BEO;
c) Follow the instructions of the members of the BEO;
d) Evacuate the building only if instructed to do so by the members of the BEO;
e) Never use elevators;



f) If the evacuation is ordered, move to the evacuation assembly area;
g) If a flash flood occurs and rising waters prevent your escape, get to a rooftop or high ground and wait for help to come to you;
h) Never try to cross a flood area on foot. The fast water could sweep you away. If you are in a car, drive very carefully. If the car stalls in a flooded area, abandon it. Many people have drowned in rising flood waters while trying to move a stalled vehicle;
i) Do not move back into the building until instructed to do so;
j) In the event of an emergency or disruption to regular operations such as inclement weather, environmental disasters, local emergencies, national emergencies, demonstrations and building occupations, employees are advised to call the CBSA Employee Notice Line at 1-866-NOTICE4 (1-866-668-4234) to obtain up-to-date information on the status of their building.










# Annexe F : Procédures d'urgence en cas d'inondation

## 1. Introduction

Les inondations représentent le risque naturel qui survient le plus fréquemment au Canada. Elles peuvent se produire à tout moment de l'année et sont le plus souvent causées par une pluie torrentielle, une fonte rapide d'un manteau neigeux épais, des embâcles ou, plus rarement, par la défectuosité d'un barrage naturel ou construit par l'homme.

Les inondations printanières sont le plus répandues dans les régions des Prairies, de l'Atlantique et du Québec en raison d'un dépassement de la capacité des réseaux fluviaux.

## 2. Définition

**Crue éclair :** crue soudaine et localisée d'un grand volume d'eau sur la terre ferme, généralement causée par des pluies exceptionnellement fortes qui peuvent atteindre leur pic en volume en l'espace de quelques minutes.

## 3. Rôles et responsabilités

### 2.1 Fonctions de l'Organisme de secours de l'immeuble (OSI)

Fonctions de l'autorité responsable de l'immeuble (ARI)

Avant une inondation

a) Vérifier si l'installation est située dans une plaine inondable en communiquant avec l'agent régional de la sécurité ainsi que les autorités locales;

b) Se renseigner sur les plans d'urgence de la communauté, les signaux d'avertissement, les voies d'évacuation et l'emplacement des refuges d'urgence;

c) Élaborer des procédures en cas d'inondation pour protéger les personnes et les équipements et les ajouter au plan d'intervention d'urgence de l'immeuble.







Pendant l'inondation

a) Communiquer avec le service d'incendie municipal ou les autorités locales pour obtenir des conseils sur la décision d'évacuer ou non l'immeuble;
b) Diriger l'intervention d'urgence pour l'immeuble;
c) S'assurer d'informer le Centre national des opérations frontalières par téléphone au ou par courriel à : boc-cof@cbsa-asfc.gc.ca.

Fonctions de l'agent de secours en chef de l'immeuble (ASCI)

Durant un avertissement d'inondation

a) Surveiller les médias électroniques pour obtenir plus d'informations sur la montée des eaux et conseiller l'autorité responsable de l'immeuble (ARI);
b) Examiner les procédures d'inondation avec les membres de l'Organisme de secours de l'immeuble et les employés clés.

Pendant l'inondation

c) S'il semble qu'une évacuation pourrait être nécessaire, communiquer avec le superviseur de l'entretien de l'immeuble pour s'assurer que les équipements de services publics, de gaz, d'électricité et d'eau sont éteints;
d) Le cas échéant, faire monter les ascenseurs à l'étage et les mettre hors tension;
e) Le cas échéant, sur l'ordre de l'ARI, diriger l'évacuation de l'immeuble conformément à la procédure d'évacuation appropriée.

Fonctions de l'agent de secours d'étage ou de son adjoint

Pendant l'inondation

a) Examiner les procédures d'inondation avec les membres de l'Organisme de secours de l'immeuble et les employés clés;
b) Attendre les directives de l'ASCI;
c) Sur l'ordre de l'ASCI, évacuer l'immeuble conformément aux procédures d'évacuation appropriées;
d) Veiller à la sécurité des employés au moment de l'évacuation de l'immeuble.

## 2.2 Obligations des employés







Pendant l'inondation

a) Demeurer calme;
b) Demeurer sur place, à moins d'indications contraires des membres de l'OSI;
c) Suivre les instructions des membres de l'OSI;
d) N'évacuer l'immeuble que sur l'ordre des membres de l'OSI;
e) Ne jamais utiliser les ascenseurs;
f) Si l'évacuation est ordonnée, se déplacer vers la zone de rassemblement en cas d'évacuation;
g) Si une crue éclair survient et que la montée des eaux empêche votre évacuation, monter sur le toit ou à un endroit surélevé et attendre que l'on vienne vous chercher;
h) Ne jamais essayer de traverser à pied un espace inondé. Le courant rapide de l'eau pourrait vous entraîner. En voiture, conduire très prudemment. En cas de panne dans un espace inondé, abandonner la voiture. Beaucoup de gens se sont noyés dans les eaux d'inondation parce qu'ils ont essayé de déplacer un véhicule en panne;
i) Ne pas retourner dans le bâtiment avant d'avoir reçu l'ordre de le faire;
j) Dans l'éventualité d'une urgence ou d'une interruption des activités habituelles, comme des intempéries, des catastrophes environnementales, des situations d'urgence d'envergure locale ou nationale, des manifestations et l'occupation de bâtiments, les membres du personnel sont invités à appeler la ligne d'information des employés de l'ASFC au 1-866-NOTICE4 (1-866-668-4234) pour obtenir des renseignements à jour sur l'état de leur immeuble.







# Appendix F1 - Flood Preparedness and Response Checklist

## 1. Purpose of this checklist

This checklist was developed to assist the Responsible Building Authority in developing flood procedures. It should be used as a guide and adapted according to the results of a risk analysis for each facility.

## 2. Planning for a flood

- ☐ Know the risk (Contact your Regional Security Office)
- ☐ Find out if your facility is located in a flood plain
- ☐ Learn the history of flooding in your area
- ☐ Find out about the elevation of your facility in relation to streams, rivers and dams
- ☐ Review your community's emergency plan and evacuation routes and where to find higher ground
- ☐ Establish warning procedures for your facility
- ☐ Establish emergency communication procedures, e.g., Alert Notification System, phone tree, etc.
- ☐ Establish and practice evacuation procedures for your facility
- ☐ Inspect the parts of your facility that are subject to flooding
- ☐ Identify records and equipment that can be moved to a higher location
- ☐ Make plans to move records and equipment if a flood occurs
- ☐ Purchase a radio and use it to listen for flood watches and warnings

## 3. Before the flood

- ☐ Review your Emergency Plan with your response team and key employees
- ☐ Take all necessary steps to prevent the release of dangerous chemicals that are stored on your property
- ☐ Locate main gas and electrical shut-offs
- ☐ Anchor all fuel tanks
- ☐ Postpone scheduled deliveries of goods
- ☐ Identify meeting place and time for all members of your Building Emergency Organization (BEO)
- ☐ Create voicemail for evacuation or out of office
- ☐ Update disaster recovery kits
- ☐ Maintain accurate inventory of products on site





- ☐ Use plugs to prevent floodwater from backing up into sewer drains, or install flood vents or flood proof barriers
- ☐ Stay tuned to local media
- ☐ Stay tuned to community messaging
- ☐ Provide an advance notice that a flood is imminent to the Border Operations Center (BOC) by phone at [redacted] or email to: boc-cof@cbsa-asfc.gc.ca.

## 4. During the flood

- ☐ Remember that life and safety take precedence over everything else
- ☐ Send non-critical staff home
- ☐ Raise elevators to the second level and turn off power
- ☐ Stay tuned to local media and evacuate as instructed or when circumstances require
- ☐ Take cell phones, charger, critical hardware and emergency kits with you
- ☐ Unplug electrical items before leaving



# Annexe F1 - Préparation aux inondations et liste de contrôle pour l'intervention

## 1. Objectif de la présente liste de contrôle

La présente liste vise à aider l'autorité responsable de l'immeuble à élaborer des procédures à suivre en cas d'inondation. Cette liste doit faire office de guide et être adaptée aux résultats de l'analyse des risques recensés pour chaque établissement.

## 2. Planification en vue d'une inondation

- ☐ Connaître le risque (communiquer avec le Bureau régional de la sécurité).
- ☐ Vérifier si l'installation est située dans une plaine inondable.
- ☐ Se renseigner sur l'historique des crues dans la région.
- ☐ Se renseigner sur l'élévation de l'installation par rapport aux ruisseaux, aux cours d'eau et aux barrages.
- ☐ Examiner le plan d'évacuation d'urgence de la communauté, les parcours d'évacuation et l'emplacement des terrains plus élevés.
- ☐ Établir des procédures d'avertissement pour l'installation.
- ☐ Établir des procédures de communication d'urgence (p. ex., système d'alerte, chaîne téléphonique).
- ☐ Établir des procédures d'évacuation pour l'installation et mener des exercices d'évacuation.
- ☐ Inspecter les parties de l'installation qui sont susceptibles d'être inondées.
- ☐ Dresser la liste des dossiers et du matériel qui peuvent être déplacés vers un emplacement plus élevé.
- ☐ Faire des plans afin de déplacer des documents et du matériel dans l'éventualité d'une inondation.
- ☐ Acheter une radio et l'utiliser pour écouter les avertissements et les veilles de crue.

## 3. Avant une inondation

- ☐ Examiner le plan d'urgence avec l'équipe d'intervention et les employés clés.
- ☐ Prendre toutes les mesures nécessaires pour empêcher le rejet de produits chimiques dangereux qui sont entreposés sur la propriété.
- ☐ Établir l'emplacement des principaux dispositifs d'arrêt des conduites de gaz et du circuit électrique.

- ☐ Ancrer tous les réservoirs de carburant.
- ☐ Reporter les livraisons prévues de marchandises.
- ☐ Établir le lieu et l'heure de rencontre avec tous les membres de l'Organisme de secours de l'immeuble (OSI).
- ☐ Créer un message vocal concernant l'évacuation ou l'absence du bureau.
- ☐ Mettre à jour les trousses de reprise après sinistre.
- ☐ Tenir un inventaire précis des produits présents sur place.
- ☐ Utiliser des clapets pour empêcher le retour des eaux de crue dans les canalisations d'égout, ou installer des drains d'évacuation ou des barrières à l'épreuve des inondations.
- ☐ Demeurer à l'écoute des médias locaux.
- ☐ Demeurer à l'écoute des messages diffusés dans la communauté.
- ☐ Informer au préalable le Centre national des opérations frontalières de l'imminence d'une inondation, par téléphone au ou par courriel à : boc-cof@cbsa-asfc.gc.ca.

## 4. Pendant l'inondation

- ☐ Se rappeler que la vie et la sécurité priment sur tout le reste.
- ☐ Renvoyer le personnel non essentiel à la maison.
- ☐ Faire monter les ascenseurs à l'étage et les mettre hors tension.
- ☐ Demeurer à l'écoute des médias locaux et évacuer en suivant les instructions ou lorsque les circonstances exigent.
- ☐ Emporter avec soi les téléphones cellulaires et les chargeurs, le matériel essentiel et les trousses d'urgence.
- ☐ Débrancher les appareils électriques avant de quitter les lieux.



# Appendix G: Tornadoes Emergency Plan Procedures

## 1. Introduction

Canada gets more tornadoes than any other country with the exception of the United States. Tornadoes are rotating columns of high winds. Sometimes they move quickly (up to 70 km/hour) and leave a long, wide path of destruction. At other times the tornado is small, touching down here and there. Large or small, they can uproot trees, flip cars and demolish houses. Tornadoes usually hit in the afternoon and early evening, but they have been known to strike at night too.Tornadoes strike suddenly. Sometimes the local electronic media will alert you to the possibility of a tornado, but usually it is their loud roaring noise that will alert you that one is coming.

Warning signs include:

- Severe thunderstorms, with frequent thunder and lightning
- An extremely dark sky, sometimes highlighted by green or yellow clouds
- A rumbling sound or a whistling sound.
- A funnel cloud at the rear base of a thundercloud, often behind a curtain of heavy rain or hail.

## 2. Roles and Responsibilities

### 2.1 Duties of employees

During a tornado:

a) Stay away from windows;
b) Take shelter in an inner hallway, room or basement;
c) Do not use an elevator;
d) Crouch down in a ditch or ravine, if caught outside and there is no suitable shelter. Get as close to the ground as possible and protect your head;
e) If driving, stop the car, get out of the vehicle, and get as close to the ground as possible. If you are caught outside and there is no shelter, crouch down in a ditch or ravine.

### 2.2 Duties of the Building Emergency Organization (BEO)

Duties of the Responsible Building Authority (RBA)

When a tornado warning is received the RBA will:





a) Co-ordinate action with other involved parties such as the Chief Building Emergency Officer, Building owner/landlord, and other tenants of the building;

When a tornado is imminent:

b) Direct emergency response;
c) Order the Chief Building Emergency Officer to move employees to shelter/safer places, staying well away from any windows until the danger has passed;
d) Order the Chief Building Emergency Officer or the Building owner/landlord to make sure electricity, gas and water is turned off;

After a tornado:

e) Contact the fire department, police and/or ambulance if necessary;
f) Order a building evacuation if necessary;
g) Activate the Business Continuity Plan(s) if the office is damaged and can no longer maintain its critical service(s) (if applicable);
h) Report the incident to Regional Security Office or in Headquarters the HQ Security Office;
i) Ensure that the Border Operations Center (BOC) is advised by phone at or by email at: boc-cof@cbsa-asfc.gc.ca.

Duties of the Chief Building Emergency Officer

a) On days where severe thunderstorms are forecasted the Chief Building Emergency Officer will listen to his/her radio for tornado warnings, instructions and information;
b) When a tornado warning is received the Chief Building Emergency Officer will advise the following personnel:
   - Responsible Building Authority;
   - Building Emergency Organization;
   - Occupational Health and Safety Committee; and
   - Building owner/landlord.
c) Make sure that electricity, gas and water are turned off;
d) If ordered by the RBA, lead the building evacuation.

Duties of the Floor Emergency Officer(s) and Deputies

a) Move employees to shelter, do not use the elevator and ensure that employees stay well away from any windows until the danger has passed;
b) If ordered by the RBA, evacuate the building when the tornado has passed, watching out for fallen debris and electric wires and proceed to a safe area away from all hazardous objects;





c) Report to the Chief Building Emergency Officer any problems encountered;
d) Render first aid as necessary;
e) Use telephones for emergency calls only.



# Annexe G : Procédures du plan d'intervention d'urgence en cas de tornades

## 1.1 Introduction

Le Canada est le pays où survient le plus grand nombre de tornades, à l'exception des États-Unis. Les tornades sont constituées de colonnes de vents violents en rotation. Certaines se déplacent rapidement (jusqu'à 70 km/h) et laissent derrière elles un long et large sillon de destruction. D'autres sont petites et ne touchent le sol qu'ici et là. Toutes les tornades, grandes ou petites, peuvent déraciner des arbres, renverser des voitures et démolir des maisons. Les tornades frappent généralement l'après-midi et en début de soirée, mais on en a déjà observé la nuit. Les tornades se forment soudainement. Les médias électroniques locaux peuvent parfois annoncer la probabilité d'une tornade, mais c'est habituellement un grondement assourdissant qui met les gens en alerte.

Signes précurseurs :

- orage violent accompagné de coups de tonnerre et d'éclairs fréquents;
- ciel très sombre, parfois parsemé de nuages verdâtres ou jaunâtres;
- grondements ou sifflements;
- nuage en forme d'entonnoir à la base d'un nuage orageux, souvent derrière un rideau de pluies torrentielles ou de grêlons.

## 2. Rôles et responsabilités

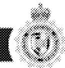
### 2.1 Obligations des employés

Pendant une tornade, les employés doivent :

a) s'éloigner des fenêtres;
b) s'abriter dans une pièce intérieure comme un couloir, une chambre ou un sous-sol;
c) éviter les ascenseurs;
d) s'ils sont dehors lorsque surpris par la tornade, s'étendre dans un fossé ou un ravin en l'absence d'un autre abri convenable, rester le plus près possible du sol et se protéger la tête;







e) s'ils sont en automobile lorsque surpris par la tornade, arrêter la voiture, sortir du véhicule et rester le plus près possible du sol; s'étendre dans un fossé ou un ravin en l'absence d'un autre abri convenable.

## 2.2 Fonctions de l'Organisme de secours de l'immeuble (OSI)

Fonctions de l'autorité responsable de l'immeuble (ARI)

Après avoir reçu un avertissement de tornade, l'autorité responsable de l'immeuble (ARI) doit :

a) coordonner l'intervention avec les autres parties concernées, dont l'agent de secours en chef de l'immeuble (ASCI), le propriétaire/locateur de l'immeuble et les autres locataires de l'immeuble.

Lorsqu'une tornade est imminente, l'ARI doit :

b) diriger l'intervention d'urgence;
c) ordonner à l'agent de secours en chef de l'immeuble (ASCI) de déplacer les employés vers un abri/un endroit sécuritaire en leur disant qu'ils doivent se tenir éloignés des fenêtres jusqu'à ce que le danger soit passé;
d) demander à l'agent de secours en chef de l'immeuble (ASCI) ou au propriétaire/locateur de l'immeuble de s'assurer de la mise hors service des réseaux de distribution de l'électricité, du gaz et de l'eau.

Après une tornade, l'ARI doit :

e) communiquer au besoin avec le service d'incendie, la police et le service ambulancier;
f) ordonner l'évacuation générale si nécessaire;
g) activer le plan ou les plans de continuité des activités si le bureau est endommagé et ne peut plus assurer le maintien des services essentiels (le cas échéant);
h) signaler l'incident à l'agent régional de la sécurité ou pour l'Administration centrale, à la Section de la sécurité de l'AC.

Fonctions de l'agent de secours en chef de l'immeuble (ASCI)

L'ASCI doit :

a) les jours où des orages violents sont prévus, se servir de sa radio à pile pour prendre connaissance des avertissements de tornade, des instructions ou d'autres renseignements;
b) si un avertissement de tornade est émis, alerter :







- l'autorité responsable de l'immeuble (ARI);
- l'Organisme de secours de l'immeuble (OSI);
- le comité de santé et de sécurité au travail;
- le propriétaire/locateur de l'immeuble.

c) s'assurer de la mise hors service des réseaux de distribution de l'électricité, du gaz et de l'eau;
d) sur l'ordre de l'ARI, diriger l'évacuation de l'immeuble.

Fonctions de l'agent ou des agents de secours d'étage (ASE) et de son/ses adjoints (AASE)

L'ASE et l'AASE doivent :

a) diriger les employés vers un abri en évitant l'ascenseur; leur dire qu'ils doivent rester éloignés de toute fenêtre jusqu'à ce que le danger soit passé;
b) sur l'ordre de l'ARI, évacuer les employés de l'immeuble après le passage de la tornade; leur dire de prendre garde aux projections de débris et aux câbles électriques et les diriger vers une zone sûre, loin d'objets dangereux;
c) signaler à l'ASCI tout problème rencontré;
d) donner les premiers soins au besoin;
e) utiliser les téléphones pour les appels d'urgence seulement.







# Appendix H: Hazardous Materials (HAZMAT) Release Procedures

## 1. Introduction

HAZMAT releases can have a major impact on the short and long-term health of CBSA employees, on service delivery, the environment and the general public. Many of our facilities are located near highways, railways, marine channels, chemical plants or industrial parks, which are often used to store, transport, transit, ship, or produce hazardous materials. Whether it is an accident involving a commercial cargo truck at a Border facility, an accidental release from a nearby chemical plant or a fuel leak from within our facilities, CBSA offices must be prepared to respond to these types of threats to protect the health and safety of employees, our clients, the neighboring public and the environment.

For each facility, HAZMAT Release Emergency Procedures should be developed based on a risk assessment and in consultation with local emergency response agencies such as police, fire department and/or HAZMAT Response Team. The plan's purpose is to prevent or limit loss of life, damage to property and impact on the environment. Since the response to these types of incidents will vary significantly depending on the situation, this document only establishes best practices.

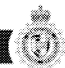
As a guiding principle, the cleanup of HAZMAT incidents is the responsibility of the individual or organization, which had ownership, management or control prior to the release. In all jurisdictions, the cost for cleanup and returning the environment to its original state is recovered under the "polluter pays" principle.

## 2. Guidelines

- The CBSA response to a HAZMAT release will depend on the situation and will be dictated by local emergency responders.
- In all incidents, local emergency agencies will strive to quickly determine the nature of the substance, the related risks, the concentration and direction of the released contaminant and the related emergency strategies for nearby residents and facilities.
- Generally, the strategies used are either Shelter in Place or Evacuation.
- Plan several evacuation routes out of the area.







- Depending on the location, some neighboring chemical industries might have audible warning systems that will alert you to potential dangers.

- CANUTEC (the Canadian Transport Emergency Centre of Transport Canada) **613-996-6666** or ***666 on a cellular phone**, is open 24/7 and accepts collect call. CANUTEC is not a responding agency; however, the services offered by CANUTEC are mostly used by emergency response teams. CBSA personnel can contact CANUTEC to get information. CANUTEC can provide immediate advice on:

  - Chemical, physical and toxicological properties and incompatibilities of dangerous goods;
  - Health hazards and first aid;
  - Fire, explosion, spill or leak hazards;
  - Remedial actions for the protection of life, property and the environment; and
  - Evacuation distances.

*** NOTE - In certain operational circumstances, Border Service Officers must call CANUTEC.

## 3. Roles and Responsibilities

### 3.1 Duties of the Building Emergency Organization (BEO)

Duties of the Responsible Building Authority (RBA)

The Responsible Building Authority (RBA) is responsible for evaluating the incident, assessing the threat and recommending, after discussion with other involved parties, the proper shelter or evacuation procedures. The RBA must:

a) Coordinate action of involved parties such as:
   i. Police, Fire department, CANUTEC, Etc.;
   ii. Chief Building Emergency Officer;
   iii. Occupational Health and Safety Committee; or
   iv. Other tenants of the building.

b) Ensure that the Border Operations Center (BOC) is advised by phone at or by email at: boc-cof@cbsa-asfc.gc.ca.

Duties of the Chief Building Emergency Officer (CBEO)

The Chief Building Emergency Officer should:







a) Implement evacuation procedures or Shelter In Place as advised by local emergency responders and RBA;
b) Contact the Occupational Health and Safety Committee; and
c) Advise your Regional Security Officer or in Headquarters the HQ Security Officer who in turn will contact the Security and Professional Standards Directorate (SPSD) at Headquarters.

### 3.2 Duties of employees

As a response strategy, evacuation is not always more efficient. Before advising people to evacuate the area, authorities will consider the type and amount of chemical released, how long it will affect the area, the length of time needed for safe evacuation, weather conditions and time of day.

#### Shelter in Place

When the evacuation is not possible or is dangerous because of dispersion of contaminants or other factors, emergency response agencies might recommend you take shelter in your home or office - "Shelter in Place."

a) Go indoors and stay there;
b) Close all outside and inside doors (creating extra barriers);
c) Close all windows;
d) Shut down Heating, Ventilation, Air Conditioning Systems (HVAC) and close all dampers;
e) Do not use kitchen or bathroom vents. Shelter in an inside room, away from windows and doors if possible;
f) Do not leave the building until informed by local authorities;
g) If possible, seal cracks around doorway with wide tape;
h) Use a damp towel or other cloth material at the bottom of the door; and
i) Listen to radio or television reports for information and further instructions.

#### Evacuation

If ordered to evacuate:

a) Evacuate the building in accordance with the local evacuation plan;







b) Evacuate immediate area using the less affected evacuation route (shortcuts may not always be the safest);
c) Stay away from routes of access of emergency responders;
d) Stay upwind from the spill or release area (avoid visible clouds);
e) Respect the minimum distance imposed by responding authorities;
f) Return to area only when authorized by local authorities; and
g) Follow local instructions concerning the safety of food and water.






Agence des services frontaliers du Canada    Canada Border Services Agency



# Annexe H - Procédures en cas de déversement de matières dangereuses

## 1. Introduction

Le déversement de matières dangereuses peut avoir des effets à court et à long termes sur la santé des employés de l'ASFC, la prestation des services, l'environnement et le public. Beaucoup de nos bureaux sont situés à proximité des routes, des chemins de fer, des chenaux, des usines chimiques ou des parcs industriels, lieux servant fréquemment à stocker, à transporter, à transiter, à expédier ou à produire des matières dangereuses. Que l'accident implique un camion de marchandises commerciales dans un poste frontalier, un déversement accidentel dans une usine voisine de produits chimiques ou une fuite de combustible dans l'une de nos installations, les bureaux de l'AFSC doivent être prêts à réagir aux menaces de ce genre afin de protéger la santé et la sécurité des employés et des clients, le public avoisinant et l'environnement.

Pour chaque installation, les procédures d'urgence en cas de déversement de matières dangereuses doivent être élaborées en fonction d'une évaluation des risques et en consultation avec des organismes d'intervention en cas d'urgence locaux comme le service de police, le service d'incendie et l'équipe d'intervention en cas de déversement de matières dangereuses. Le plan a pour but de prévenir ou de limiter les pertes de vies, les dommages aux biens et les répercussions sur l'environnement. Comme l'intervention dans ces incidents variera grandement selon la situation, le présent document ne contient que des pratiques exemplaires.

Comme principe directeur, le nettoyage des déversements de matières dangereuses doit être pris en charge par le particulier ou l'organisation qui était propriétaire des matières en cause ou qui en assurait la gestion ou le contrôle avant le déversement. Toutes les administrations prévoient que le coût du nettoyage et du rétablissement de l'environnement dans son état original est recouvré conformément au principe du pollueur-payeur.

## 2. Lignes directrices

- La réaction de l'ASFC dépendra de la situation et sera dictée par les intervenants locaux.
- Dans tous les incidents, les organismes d'urgence locaux s'efforceront de déterminer rapidement la nature de la matière dangereuse, les risques qu'elle présente, la







concentration et la propagation des contaminants déversés et les stratégies d'urgence connexes pour les résidents et les installations du voisinage.

- En règle générale, les stratégies utilisées sont le regroupement dans un abri sur place ou l'évacuation.

- Planifier plusieurs chemins d'évacuation du secteur.

- Dans certains emplacements, les usines voisines de produits chimiques pourraient avoir des systèmes d'alerte sonores qui vous mettent en garde contre les dangers éventuels.

- CANUTEC (le Centre canadien d'urgence transport de Transports Canada), **613-996-6666**, ou ***666 sur un téléphone cellulaire**, est ouvert tous les jours, 24 heures sur 24, et accepte les appels sans frais. CANUTEC n'est pas un organisme d'intervention; cependant, les services offerts par CANUTEC sont pour la plupart utilisés par les équipes d'intervention d'urgence. Le personnel de l'ASFC peut communiquer avec CANUTEC pour obtenir des renseignements. CANUTEC peut fournir des conseils immédiats au sujet des aspects suivants :

    - les propriétés chimiques, physiques et toxicologiques et les incompatibilités des matières dangereuses;
    - les risques pour la santé et les premiers secours;
    - les risques d'incendie, d'explosion, de déversement ou de fuite;
    - les mesures correctives à prendre pour protéger la vie, les biens et l'environnement;
    - les superficies à évacuer.

*** REMARQUE : Dans certaines circonstances opérationnelles, les agents des Services frontaliers doivent appeler CANUTEC.

## 3. Rôles et responsabilités

### 3.1 Fonctions de l'Organisme de secours de l'immeuble (OSI)

Fonctions de l'autorité responsable de l'immeuble (ARI)

Il incombe à l'autorité responsable de l'immeuble d'évaluer les circonstances de l'incident, d'évaluer la menace et de recommander, avec l'avis d'autres parties concernées, les procédures à suivre pour une évacuation ou le regroupement dans un abri, c'est-à-dire. L'ARI doit :







a) coordonner l'intervention des parties concernées, soit :
   i. les services de police, les services d'incendie, CANUTEC, etc.;
   ii. l'agent de secours en chef de l'immeuble;
   iii. le comité de santé et de sécurité au travail;
   iv. les autres locataires de l'immeuble.

b) S'assurer d'informer le Centre national des opérations frontalières par téléphone au ou par courriel à : boc-cof@cbsa-asfc.gc.ca.

Fonctions de l'agent de secours en chef de l'immeuble (ASCI)

L'agent de secours en chef de l'immeuble doit :

a) mettre en œuvre les procédures d'évacuation ou de regroupement dans un abri sur place selon les directives données par les intervenants locaux et l'ARI;
b) communiquer avec le comité de santé et de sécurité au travail;
c) aviser l'agent régional de la sécurité ou pour l'Administration centrale, l'agent de la sécurité de l'AC, qui, à son tour, avisera la Direction de la sécurité et des normes professionnelles (DSNP), à l'Administration centrale.

**3.2 Obligations des employés**

L'évacuation n'est pas toujours la mesure la plus efficace. Avant d'indiquer aux personnes d'évacuer le secteur, les autorités tiendront compte du type et de la quantité du produit chimique déversé, de la durée de ses effets sur le secteur, du temps qu'exigera l'évacuation, des conditions météorologiques et du moment de la journée.

**Abri sur place**

Lorsque l'évacuation n'est pas possible ou est dangereuse en raison de la dispersion des contaminants et d'autres facteurs, les organismes d'intervention peuvent recommander aux occupants de se regrouper dans un « abri sur place » à l'intérieur de la maison ou du bureau en procédant comme suit :

a) aller à l'intérieur et y demeurer;
b) fermer toutes les portes à l'intérieur et donnant sur l'extérieur pour créer des barrières additionnelles;
c) fermer toutes les fenêtres;
d) fermer le système de chauffage, de ventilation et de climatisation et fermer tous les clapets;





e) ne pas utiliser la hotte de cuisine ou le ventilateur de la salle de bains, s'abriter dans une pièce intérieure et se tenir loin des fenêtres et des portes s'il y a lieu;
f) ne pas quitter l'immeuble avant d'avoir reçu l'avis des autorités locales;
g) lorsque c'est possible, utiliser du ruban adhésif pour calfeutrer les fentes des portes;
h) placer une serviette ou un autre tissu humide au bas de la porte;
i) écouter la radio ou regarder la télévision pour obtenir de l'information et des instructions.

**Évacuation**

Si l'ordre d'évacuation est donné, procéder comme suit :

a) évacuer l'immeuble conformément au plan d'évacuation;
b) évacuer le secteur immédiat en utilisant les chemins d'évacuation les moins touchés (les raccourcis ne sont pas toujours les plus sûrs);
c) s'éloigner des voies d'accès utilisées par les intervenants d'urgence;
d) se tenir en amont du déversement ou du lieu de déversement (s'éloigner des nuages visibles);
e) respecter les distances minimales imposées par les intervenants;
f) regagnez l'endroit où vous étiez lorsque les autorités locales vous autorisent à le faire;
g) suivre les instructions locales liées à la salubrité des aliments et de l'eau.



# Appendix I: Public Health Hazard Procedures

## Introduction:

1. In recent years, public health hazards have received increased attention from the media and the public. Incidents such as the Walkerton water contamination or the arrival of the West Nile Virus in Southern Ontario have generated increased public awareness of the potential for serious harm to communities and their infrastructure.

2. Because of Canada's vast geographical area and demographics, the capability of communities to deal with such hazards will vary from location to location.

## Responsibility

3. Although government officials at all levels consult and coordinate response to such incidents, the main responsibility for managing these types of hazards rests with local health officials. Should the scope of the incidents overwhelm local health officials and their resources, the involvement of the provincial or the federal governments (Health Canada) can be requested.

4. Although the Canada Border Services Agency (CBSA) is not responsible for primary response and would not usually be actively involved in managing a public health hazard, we could; however, be subject to major operational impacts should such an incident occur, which affect our employees, partners or clients.

5. In such an event, the CBSA emergency structure would be activated to ensure a timely and coordinated approach to managing the crisis. The Regional Operations Centre (ROC) in the affected area would be opened, and would coordinate with the Border Operations Centre (BOC) at Headquarters.

## Points to remember

6. The CBSA emergency structure is set up to provide rapid response to emergency events, and to manage security and operational issues, as well as meeting human needs resulting from the critical event.



7. The Operations Branch is responsible for managing the BOC and maintaining established emergency contacts with many federal departments and agencies in order that we may respond quickly, with the needed resources.

## How to react

8. Do not panic. Although these types of events can be alarming, such a response will inhibit your reaction and thought processes. Make a conscious decision to remain calm.

9. Stay informed. For major events, the media (T.V., radio) is usually the most effective tool used by emergency responders and officials to broadcast further warnings or situation updates.

10. Local Health officials will broadcast health advisories, including: situational updates, special instructions, routes and means of exposure (respiratory system, skin and mucous membranes or digestive system), contaminated sources, prevention or mitigation strategies and available treatments and treatment centres.

11. Local officials will also broadcast important information on food and supply availability and if required, distribution centres.

12. Follow the instructions provided by emergency response organizations and stay in contact with your office for operational instructions.







# Annexe I : Procédures en cas de menace contre la santé publique

## Introduction

1. Au cours des dernières années, les menaces contre la santé publique ont reçu une attention croissante de la part des médias et du public. Des incidents tels que la contamination de l'eau à Walkerton et l'arrivée du virus du Nil dans le sud de l'Ontario ont grandement sensibilisé le public aux dommages graves que peuvent subir les collectivités et leurs infrastructures.

2. La capacité à intervenir face à ces risques varie selon les collectivités en raison de la vaste superficie géographique du Canada et de la répartition de la population.

## Responsabilité

3. Les représentants des gouvernements de tous les paliers se consultent pour coordonner la réaction aux incidents de ce genre; toutefois, les autorités sanitaires locales demeurent les principales responsables de la gestion des menaces de ce type. Si l'incident est d'une ampleur qui dépasse les capacités et les ressources des responsables locaux de la santé, la municipalité peut demander l'aide du ministère de la Santé fédéral ou provincial.

4. L'ASFC n'est pas chargée de réagir à une menace contre la santé publique et n'interviendrait pas habituellement, de façon active, dans la gestion d'une telle menace. Cependant, elle pourrait avoir à composer avec des répercussions opérationnelles importantes si un incident donné se produisait et touchait ses employés, ses partenaires ou ses clients.

5. Dans ce cas, l'organisation d'urgence de l'ASFC serait activée afin de garantir la gestion rapide et coordonnée de la crise. Le Centre régional des opérations (CRO) de la région touchée serait ouvert et coordonnerait la crise avec le Centre des opérations frontalières (COF) à l'Administration centrale.

## Consignes

6. La structure d'intervention d'urgence de l'ASFC permet de réagir rapidement aux urgences, de gérer les questions relatives à la sécurité et aux opérations et de combler les besoins des personnes découlant de la situation d'urgence.

7. La Direction générale des opérations est chargée de gérer le COF et de maintenir les communications d'urgence avec un grand nombre de ministères et d'organismes fédéraux afin d'être en mesure de réagir rapidement et d'affecter les ressources nécessaires.



## Comment réagir

8. Rester calme. Ces événements peuvent être alarmants, et céder à la panique peut nuire à la réaction et au processus cognitif. Il convient de prendre rationnellement la décision de rester calme.

9. Demeurer informé. En cas d'événement majeur, les médias (télévision et radio) sont habituellement l'outil le plus efficace que peuvent utiliser les intervenants d'urgence et les autorités pour diffuser d'autres avertissements et faire le point sur la situation.

10. Les autorités sanitaires locales diffuseront des conseils sanitaires, notamment des rapports d'étape sur la situation, des instructions spéciales et des informations sur les voies et les moyens d'exposition (système respiratoire, peau et muqueuse, système digestif), les sources contaminées, les stratégies de prévention ou de protection, les traitements disponibles et les centres de traitement.

11. Les responsables locaux diffuseront également de l'information importante sur la nourriture et les stocks disponibles ainsi que sur les centres de distribution s'il y a lieu.

12. Suivre les instructions données par les organismes d'intervention en cas d'urgence et demeurer en contact avec son bureau afin d'obtenir les instructions opérationnelles.







# Appendix J: Major Crisis Incidents – Guidelines

## 1. Introduction

Sometimes, incidents happen where no mitigation or prevention strategy can stop the destruction. Like the terrorist attacks of September 11, 2001, against the World Trade Center and the Pentagon, these calamitous events can have major, long-term psychological and financial impact. The destruction and shock can be so great that managers, employees and clients are overwhelmed and uncertainty can quickly give way to widespread panic.

This document describes the essential elements in place that will serve to reassure managers and employees of the Canada Border Services Agency (CBSA), should they encounter such an event.

## 2. Points to remember

Everyone should be aware that all levels of government, including municipal, provincial and federal departments and agencies, have plans in place that allow rapid response to these types of crises. Supported by certain legislation, such as the *Emergencies Act* and the *Emergency Preparedness Act*, the federal government has many resources from which to draw in order to manage such events. The Federal Emergency Response Plan (FERP) coordinates the response activities of all federal government institutions in the event of a catastrophic event that overwhelms the resources of provinces and municipalities

The CBSA emergency structure is set up to provide rapid response to these types of events and to manage security and operational issues, as well as providing for human needs resulting from the critical event.

The CBSA has established emergency contacts with many federal departments and agencies, enabling rapid response with the needed resources.

## 3. How to react

Do not panic. Stay calm. Although these types of events can quickly lead to widespread panic, such a response will inhibit your reaction and thought processes.

Evacuate the immediate area and gather in a safe, secure area. Bystanders are often injured.

If you are injured, seek immediate medical attention. Even though the injury may be severe, adrenaline will sometimes subdue or reduce the feeling of pain. Do not underestimate your injuries. Listen to emergency workers and accept their advice.





Many individuals will feel the need to contact and reassure family members. Because telecommunications, both cellular and landlines will be subject to high traffic, a busy signal is very probable.

Listen to local media reports. For major events, the media (T.V., radio) is usually the most effective tool used by emergency responders to broadcast further warnings or situation updates. Follow instructions provided by emergency response organizations.

Employees are advised to call 1-866-notice4 (1-866-668-4234) in the event of an emergency or disruption to regular operations. Examples of emergency or disruption to regular operations include: inclement weather, environmental disasters, local emergencies, national emergencies, demonstrations and building occupations.



# Annexe J - Crises majeures – Lignes directrices

## 1. Introduction
Il arrive parfois que des incidents surviennent sans qu'aucune stratégie d'atténuation ou de prévention ne puisse empêcher la destruction qu'ils provoquent. À l'instar des attaques terroristes du 11 septembre 2001 contre le World Trade Center et le Pentagone, ces événements catastrophiques ont une incidence psychologique et financière à long terme. La destruction et le choc peuvent être énormes au point où les gestionnaires, les employés et les clients sont dépassés par les événements. L'incertitude peut rapidement s'installer et les gens peuvent céder à la panique.

Le présent document décrit les éléments essentiels mis en place pour aider les gestionnaires et les employés de l'Agence des services frontaliers du Canada (ASFC) à faire face à de tels événements.

## 2. Consignes
Tous les ordres de gouvernement, y compris les administrations municipales, les ministères et organismes provinciaux et fédéraux, disposent de plans d'intervention rapide en cas de crises majeures. De plus, le gouvernement fédéral peut, en vertu de la *Loi sur les mesures d'urgence* et de la *Loi sur la protection civile*, faire appel à différentes ressources pour la gestion de tels événements. Le Plan fédéral d'intervention d'urgence (PFIU) coordonne les activités d'intervention de toutes les institutions fédérales en cas de catastrophe où les ressources municipales et provinciales disponibles ne suffisent plus.

L'organisation d'urgence de l'ASFC est structurée pour assurer une intervention rapide en cas de crises majeures, gérer des questions d'ordre sécuritaire et opérationnel et répondre aux besoins humains résultant de tels événements.

L'ASFC a dressé une liste de personnes issues de nombreux ministères et organismes fédéraux avec qui communiquer pour obtenir les ressources nécessaires à une intervention rapide.

## 3. Comment réagir
Ne pas paniquer. Rester calme. Les événements de ce genre peuvent provoquer rapidement une panique généralisée et inhiber le processus de réaction et de réflexion des personnes qui en sont victimes.

Évacuer la zone immédiate et se diriger vers un lieu sûr. Les blessures sont fréquentes parmi les spectateurs.







En cas de blessures, il faut immédiatement tenter d'obtenir des soins. La blessure peut être grave, mais l'adrénaline atténue ou réduit parfois la douleur. Ne pas sous-estimer la gravité d'une blessure. Écouter les intervenants d'urgence qualifiés et accepter leurs conseils.

De nombreuses personnes voudront communiquer avec des membres de leur famille pour les rassurer. Or, celles qui tentent de le faire obtiendront fort probablement une tonalité d'occupation puisque les réseaux de télécommunication, dont les téléphones cellulaires ou les lignes terrestres, seront très achalandés.

Écouter les reportages des médias locaux. En cas de crises majeures, les médias (télévision et radio) sont habituellement les outils les plus efficaces à la disposition des intervenants d'urgence pour diffuser d'autres avertissements ou pour faire le point sur la situation. Suivre les instructions fournies par les organismes d'intervention d'urgence.

Les employés doivent avoir recours au numéro 1-866-notice4 (1-866-668-4234) dans un cas d'urgence ou de perturbation des opérations régulières. Voici des exemples d'une telle situation : intempéries, désastres environnementaux, urgences locales, urgences nationales, manifestations et occupations d'édifice.







# Appendix K: Demonstrations and Occupations - Guidelines

## 1. Introduction

Demonstrations and occupations of public premises are increasingly relied upon as a means of expressing views and exercising political pressure. They can occur in any location, at any time. Managers should be prepared to respond to demonstrations and occupations to protect employees, assets, clients and the public in general and must take all reasonable measures during a demonstration to prevent an occupation of Canada Border Service Agency (CBSA) premises.

## 2. Before a Demonstration or an Occupation

The Responsible Building Authority (RBA) will contact the police service that has jurisdiction to develop a general action plan in anticipation of such situations. The plan should be prepared based on police recommendations.

Where there is information or intelligence regarding a pending demonstration, consultation must be held with the local police for assistance in preparing a plan specific to the situation.

Other parties should also be involved, such as the Border Operations Centre (BOC) Regional Security Office or in Headquarters the HQ Security Section, Legal Services, Department of Justice, the Regional Director General and the Vice President of the affected program area if the issue under protest is relevant to their business line.

When CBSA is not the main tenant and when other departments or agencies occupy the building, the most senior official of the CBSA will communicate with the other tenants.

If a protest is not directed at CBSA, the most senior official of the department or agency in which the protest and occupation is aimed at, will usually handle the situation. If the demonstration or the occupation affects CBSA employees, and clients, health and safety and assets, the most senior official within CBSA will activate the emergency plan for these types of situations, in coordination or consultation with the Responsible Building Authority.

## 3. Roles and Responsibilities

### 3.1 Duties of the Building Emergency Organization (BEO)







Duties of the Responsible Building Authority (RBA)

**During a Demonstration:**

a) Take all reasonable measures during a demonstration to prevent an occupation of CBSA premises;
b) Call the police service that has jurisdiction. The RCMP will intervene only if a federal minister is present in the building and the Minister's life could be in danger;
c) Determine the reason for the demonstration, either from picket information or by talking with demonstrators;
d) Inform the BOC and the Workplace Health and Safety Committee;
e) Report to the Regional Security Office or in Headquarters the HQ Security Section who in turn will contact the Security and Professional Standards Directorate (SPSD) at Headquarters (HQ) at the earliest possible opportunity.

**During an Occupation:**

a) Call the police service that has jurisdiction;
b) Take the necessary measures to assure the removal of all participants in an occupation of a CBSA premise;
c) Have in hand the building emergency plan for occupations of CBSA premises;
d) Report to the Regional Security Officer or in Headquarters the HQ Security Section who in turn will contact the SPSD at HQ at the earliest possible opportunity;
e) If demonstrators appear at any time to endanger an employees' physical well-being, have the employees removed to another floor or another building. As a measure of last resort, the RBA is authorized to close the office, under the following conditions and with proper notification:
    - When there is strong reason to believe that maintaining operations could jeopardize the safety and security of employees and/or the public; or
    - When there is strong reason to believe that maintaining operations could bring about damage to government property.

**Non-Disruptive Occupations:**

a) If the Responsible Building Authority (RBA), after consultations, is satisfied that the occupation will not disrupt the office business, or if he/she is prepared to treat the occupation in this way, initially he/she should be guided by the following points:
    - Ensure that the demonstrators understand they must leave prior to closing time and that they must not obstruct the work of the office;







- Inform the police service having jurisdiction that the occupation is being treated as non-disruptive. The police are to be asked to provide on-site support; and,
- Take action to have demonstrators removed by police if at the end of the day, the demonstrators refuse to leave or if during the day they disrupt the office business.

**Disruptive Occupations:**

a) Based on discussion with the demonstrators and/or intelligence reports, the RBA can satisfactorily determine if an occupation disrupts or is likely to disrupt the work of the office, he/she should be guided by the following:
   - Contact police service having local jurisdiction to determine if they are prepared to remove the demonstrators;
   - If the police are prepared to assist, the RBA will inform the demonstrators that they are interfering with the operation of the office and that this cannot be tolerated. They are to be warned that if they do not leave voluntarily, the police will be called in; and
   - If the police do not wish to proceed with the removal of the demonstrators, the possibility of filing for an injunction will be discussed with Legal Services.

**Silent Hours Occupations:**

a) Although there may be compelling reasons to take measures for the immediate expulsion of individuals occupying premises after hours, the matter is not without some difficulty at law. Measures considered and taken will depend on how the situation evolves. Once again, if the police do not want to proceed with the removal of the demonstrators, the possibility of filing for an injunction will be discussed with Legal Services.

**Actions to be taken after a Demonstration or an Occupation:**

a) Search premises thoroughly to ensure that all demonstrators have been removed or left voluntarily; check for unusual items and alert the police if anything suspicious is found;
b) Re-establish perimeter security;
c) Take inventory of material and assess losses and damages, if any;
d) Record and report all suspicious and improper occurrences and assist the police as necessary or take appropriate action;
e) Take photos, as necessary; and
f) Review and update the building emergency plan, if necessary;
g) Report the details to the Regional Security Officer or in Headquarters the HQ Security Section who in turn will contact SPSD at HQ.

Duties of the Chief Building Emergency Officer (CBEO)



a) Alert the Floor Emergency Officers;
b) Advise the Workplace Health and Safety Committee;
c) Contact the Deputy Building Emergency Officer;
d) Alert other building occupants;
e) Assist the RBA in directing the emergency.

Duties of the Floor Emergency Officer(s) and Deputies

a) Assist the RBA and the CBEO.

**3.2 Duties of employees**

During an occupation or demonstration, employees must:

Not intervene or attempt to remove any demonstrator;

- Not become involved in any activities of the demonstrators;
- Avoid needless aggravation of the demonstrators;
- Follow instructions given by the members of the Building Emergency Organization; and
- Safeguard all sensitive information and assets by removing such from the immediate area or by locking all containers.







# Annexe K : Manifestations et occupations – Lignes directrices

## 1. 1 Introduction

Les manifestations, de même que l'occupation des établissements publics, sont de plus en plus utilisées comme un moyen d'exprimer des opinions et d'exercer des pressions politiques. Elles peuvent se produire à n'importe quel endroit ou moment. Les gestionnaires devraient être prêts à réagir aux manifestations et aux occupations afin de protéger les employés, les biens, les clients et le public en général. Durant une manifestation, ils doivent prendre toutes les mesures raisonnables pour empêcher l'occupation des locaux de l'Agence des services frontaliers du Canada (ASFC).

## 2. Avant une manifestation ou une occupation

L'autorité responsable de l'immeuble (ARI) doit communiquer avec le service de police compétent pour élaborer un plan d'action général en prévision de telles situations. Le plan devrait être élaboré selon les recommandations de la police.

Lorsqu'on reçoit de l'information concernant une manifestation imminente, on doit consulter le service de police pour obtenir de l'aide en vue de l'élaboration d'un plan propre à la situation.

D'autres parties devraient également être mises à contribution, comme le Centre des opérations frontalières (COF), le Bureau régional de la sécurité ou pour l'Administration centrale, la Section de la sécurité de l'AC, les Services juridiques, le ministère de la Justice, le directeur général régional et le vice-président du programme touché si la question à l'origine de la manifestation relève de leur secteur d'activités.

Si l'ASFC n'est pas le locataire principal et que d'autres ministères et organismes occupent l'immeuble, le plus haut fonctionnaire de l'ASFC dans l'immeuble doit communiquer avec les autres locataires.

Si l'ASFC n'est pas visée directement par la manifestation, le titulaire du poste le plus important du ministère ou de l'organisme visé se chargera habituellement de la situation. Si la manifestation ou l'occupation porte préjudice à la santé et à la sécurité des employés et des clients de l'ASFC et aux biens de celle-ci, le plus haut fonctionnaire de l'ASFC dans l'immeuble activera le plan d'urgence pour les situations de ce genre, en coordination et en consultation avec l'autorité responsable de l'immeuble (ARI).







# 3. Rôles et responsabilités

## 3.1 Fonctions de l'Organisme de secours de l'immeuble (OSI)

Fonctions de l'autorité responsable de l'immeuble (ARI)

**Durant une manifestation, l'ARI doit :**

a) prendre toutes les mesures raisonnables pour empêcher l'occupation des locaux de l'ASFC;
b) appeler les services de police compétents. La GRC interviendra uniquement si un ministre fédéral se trouve dans l'immeuble et que sa vie pourrait être en danger;
c) déterminer le but de la manifestation à partir de l'information sur les pancartes ou en parlant à des manifestants;
d) informer le Centre des opérations frontalières (COF) et le comité de santé et de sécurité au travail;
e) aviser le Bureau régional de la sécurité ou pour l'Administration centrale, la Section de la sécurité de l'AC, qui, à son tour, avisera dans les plus brefs délais la Direction de la sécurité et des normes professionnelles (DSNP), à l'Administration centrale.

**Durant une occupation, l'ARI doit :**

a) appeler les services de police compétents;
b) prendre toutes les mesures requises pour évacuer ou faire évacuer les locaux de l'ASFC occupés par les manifestants;
c) avoir à portée de la main le plan d'intervention d'urgence de l'immeuble pour les cas d'occupation des locaux de l'ASFC;
d) aviser l'agent régional de la sécurité ou pour l'Administration centrale, la Section de la sécurité de l'AC, qui à son tour, avisera dans les plus brefs délais la Direction de la sécurité et des normes professionnelles (DSNP), à l'Administration centrale;
e) si, à un moment donné, les manifestants semblent sur le point de mettre en danger le bien-être physique des employés, diriger ceux-ci vers un autre étage ou un autre immeuble et, en dernier recours, fermer le bureau avec une notification appropriée et dans les conditions suivantes :
   - lorsqu'elle a de solides motifs de croire que le maintien des opérations pourrait mettre en danger la sécurité des employés ou du public;



- lorsqu'elle a de solides motifs de croire que le maintien des opérations pourrait entraîner des dommages aux biens de l'État.

**Durant une occupation non perturbatrice, l'ARI doit :**

a) envisager de suivre les procédures initiales suivantes si, après consultation, elle est convaincue que l'occupation ne perturbera pas les activités du bureau ou prête à gérer la situation comme une occupation non perturbatrice :
   - s'assurer que les manifestants savent qu'ils doivent quitter les locaux avant la fermeture et qu'ils ne doivent pas nuire au travail dans le bureau;
   - informer le service de police compétent que l'occupation est considérée comme étant non perturbatrice; demander au service de police s'il est prêt à fournir un soutien sur place au besoin;
   - prendre des mesures afin que la police expulse les manifestants à la fin de la journée s'ils refusent de partir ou durant la journée s'ils perturbent le travail.

**Durant une occupation perturbatrice, l'ARI doit :**

a) envisager de suivre les procédures suivantes si, d'après une discussion avec des manifestants ou la consultation de rapports de renseignements, elle détermine de manière satisfaisante que l'occupation perturbe ou pourrait perturber les activités du bureau :
   - communiquer avec le service de police compétent afin de savoir s'il est prêt à évacuer les manifestants au besoin;
   - si le service de police est prêt à fournir un soutien sur place, informer les manifestants qu'ils gênent les activités du bureau, qu'une telle situation ne peut être tolérée et que police sera appelée sur les lieux s'ils ne quittent pas volontairement les locaux;
   - discuter avec les Services juridiques de la possibilité d'obtenir une injonction si la police ne veut pas intervenir.







## Occupations durant les heures de fermeture

a) Bien qu'il puisse exister des raisons impérieuses de prendre des mesures en vue de l'expulsion immédiate d'individus occupant les locaux après les heures d'ouverture, cette question soulève certaines difficultés d'ordre juridique. Les mesures envisagées et prises sont fonction de l'évolution de la situation. La police peut décider de ne pas expulser les manifestants et on devra alors étudier avec les Services juridiques la possibilité de demander une injonction.

## Mesures à prendre après une manifestation ou une occupation

a) Ratisser les locaux afin de s'assurer que tous les manifestants ont été expulsés ou sont partis volontairement; porter attention aux articles inhabituels et alerter la police si un objet suspect est trouvé;
b) rétablir la sécurité du périmètre;
c) dresser la liste du matériel et des biens perdus ou endommagés, s'il y a lieu;
d) consigner et signaler les incidents suspects ou inconvenants, aider au besoin la police ou prendre les mesures appropriées;
e) au besoin, prendre des photos;
f) au besoin, examiner et mettre à jour le plan d'intervention d'urgence de l'immeuble;
g) communiquer les détails à l'agent régional de la sécurité ou pour l'Administration centrale, la Section de la sécurité de l'AC, qui à son tour, avisera la Direction de la sécurité et des normes professionnelles (DSNP), à l'Administration centrale.

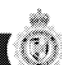
Fonctions de l'agent de secours en chef de l'immeuble (ASCI)

L'ASCI doit :

a) alerter les agents de secours d'étage;
b) aviser le comité de santé et de sécurité au travail;
c) communiquer avec l'adjoint de l'agent de secours en chef de l'immeuble (AASCI);
d) alerter les autres occupants de l'immeuble;
e) aider l'ARI dans la gestion de l'urgence.







Fonctions de l'agent ou des agents de secours d'étage (ASE) et de son/ses adjoints (AASE)

L'ASE et l'AASE doivent :

a) aider l'ARI et l'ASCI.

## 3.2 Obligations des employés

Durant une occupation ou une manifestation, les employés doivent :

- éviter d'intervenir ou de tenter d'expulser un manifestant;
- éviter de s'impliquer dans l'une ou l'autre activité des manifestants;
- éviter d'aggraver inutilement le comportement des manifestants;
- suivre les instructions données par les membres de l'Organisme de secours de l'immeuble (OSI);
- protéger les renseignements et les biens de nature délicate en les retirant du secteur immédiat ou en verrouillant tous les classeurs.





Canada Border Services Agency | Agence des services frontaliers du Canada



# Appendix K1 - Responsible Building Authority Checklist – Occupation

| **Be sure the following actions have been taken** | **√** | **Time Actioned** |
|---|---|---|
| Call local police force | | |
| Notify the Border Operations Centre (BOC) | | |
| Contact the Regional Security Office or in Headquarters the HQ Security Section | | |
| Activate the Emergency Operations Centre | | |
| Notify the Chief Building Emergency Officer | | |
| Verify the reason for the occupation | | |
| Inform the demonstrators that the police have been called | | |
| Consult with other authorities (bridge or port authority, US Customs) or tenants | | |
| Remove waste receptacles and other objects if possible or secure them (inside and outside) | | |
| Assign someone to ensure the safety of restricted access areas | | |
| Notify employees of situation and give instructions | | |
| Remove employees from affected area (if necessary) | | |
| Assign someone to control and direct incoming and outgoing traffic or, | | |
| Assign someone to turn away visitors | | |
| Contact the Workplace Health and Safety Committee | | |
| Contact Legal Services and or Justice if required for legal advice. | | |
| Make sure an incident report is completed | | |







# Annexe K1 - Autorité responsable de l'immeuble – Liste de contrôle – Manifestations

| S'assurer que les mesures suivantes ont été prises | √ | Heure d'exécution |
|---|---|---|
| Appeler le service de police local | | |
| Communiquer avec le Centre des opérations frontalières (COF) | | |
| Communiquer avec le Bureau régional de la sécurité ou pour l'Administration centrale, avec la Section de la sécurité de l'AC | | |
| Aviser l'agent de secours en chef de l'immeuble | | |
| Activer le centre des opérations d'urgence | | |
| Vérifier le motif de la manifestation | | |
| Affecter une personne au lobby pour qu'elle surveille la situation | | |
| Mettre au courant les employés et leur donner des instructions | | |
| Enlever ou protéger les poubelles à l'extérieur | | |
| Surveiller les terrains de stationnement relevant de la responsabilité de l'ASFC | | |
| S'assurer que la santé et la sécurité des personnes qui entrent dans l'immeuble ou qui en sortent ne sont pas menacées | | |
| Communiquer avec le comité de santé et de sécurité au travail | | |
| Prendre les mesures raisonnables pour prévenir l'occupation de l'immeuble | | |
| Filmer la manifestation, au besoin, au moyen d'une caméra vidéo | | |
| S'assurer qu'un rapport d'incident est rempli | | |










# Appendix K2 - Responsible Building Authority Checklist – Occupation

| Be sure the following actions have been taken | √ | Time Actioned |
|---|---|---|
| Call local police force | | |
| Notify the Border Operations Centre (BOC) | | |
| Contact the Regional Security Office or in Headquarters the HQ Security Section | | |
| Activate the Emergency Operations Centre | | |
| Notify the Chief Building Emergency Officer | | |
| Verify the reason for the occupation | | |
| Inform the demonstrators that the police have been called | | |
| Consult with other authorities (bridge or port authority, US Customs) or tenants | | |
| Remove waste receptacles and other objects if possible or secure them (inside and outside) | | |
| Assign someone to ensure the safety of restricted access areas | | |
| Notify employees of situation and give instructions | | |
| Remove employees from affected area (if necessary) | | |
| Assign someone to control and direct incoming and outgoing traffic or, | | |
| Assign someone to turn away visitors | | |
| Contact the Workplace Health and Safety Committee | | |
| Contact Legal Services and or Justice if required for legal advice. | | |
| Make sure an incident report is completed | | |





Agence des services frontaliers du Canada | Canada Border Services Agency



# Annexe K2 - Liste de vérification de l'autorité responsable de l'immeuble (ARI) – Occupation

| S'assurer que les mesures suivantes ont été prises | √ | Heure d'exécution |
|---|---|---|
| Appeler le service de police local. | | |
| Avertir le Centre des opérations frontalières (COF). | | |
| Communiquer avec le Bureau régional de la sécurité ou pour l'Administration centrale, avec la Section de la sécurité de l'AC | | |
| Activer le centre des opérations d'urgence. | | |
| Aviser l'agent de secours en chef de l'immeuble. | | |
| Vérifier le motif de l'occupation. | | |
| Aviser les manifestants qu'on a appelé le service de police. | | |
| Mener des consultations avec les autres administrations (administration des ponts ou portuaire, service des douanes américaines) ou locataires. | | |
| Enlever s'il y a lieu les poubelles et autres objets ou les protéger (à l'intérieur et à l'extérieur). | | |
| Affecter une personne à la sécurité des zones à accès contrôlé. | | |
| Mettre au courant les employés et leur donner des instructions. | | |
| Faire sortir les employés du secteur touché (au besoin). | | |
| Affecter une personne pour qu'elle se charge de contrôler et de guider les allées et venues. | | |
| Affecter une personne pour qu'elle refuse l'entrée aux visiteurs. | | |
| Communiquer avec le comité de santé et de sécurité au travail. | | |
| Communiquer avec les Services juridiques et/ou le ministère de la Justice pour obtenir un avis juridique. | | |
| S'assurer qu'un rapport d'incident est rempli. | | |







# Building Emergency Response Planning
## Appendix L: Lockdown Procedures

### 1. Introduction

A lockdown should only be used when there is a major incident or threat of violence **within** the building, or in relation to the building. In this situation, employees should cease work and gather in a room that can be locked from the inside and await further instructions from senior building officials, or law enforcement officials.

### 2. Communication

If a situation possibly requiring a lockdown is discovered, the following communication procedures should be followed:

- The individual making the discovery should immediately call **9-1-1** if safe to do so;
- If possible, contact a manager, a Regional or Headquarters (HQ) Security Officer, or an on-site Floor Emergency Officer and provide as much information as possible;
- An emergency lockdown will usually be first announced by intercom, voice communication or other readily available means;
- Fire evacuation alarms are **not** to be sounded;
- Once alerted as to a lockdown, individuals should be advised to refrain from using personal cellphones and should follow any instructions issued by the Departmental Security Officer (DSO), management, a Regional or HQ Security Officer, or the on-site Floor Emergency Officer; and
- Available information should be quickly communicated by the DSO, Chief Building Emergency Officer, Deputy Chief Building Emergency Officer or alternate to the Regional or HQ Security Officer and local police authorities.

### 3. Roles and Responsibilities

#### 3.1 Duties of Employees

As part of lockdown procedures, occupants should be informed to undertake the following actions:

a) Call 911 and if safe to do so notify a Manager, or Security.
b) **DO NOT** pull/activate fire alarm.
c) Immediately lock yourself in your office or the closest room. If the room cannot be locked, barricade it with furniture. If the room has no door, hide under a desk or where you cannot be seen.
d) Move to a safe corner to reduce visibility – keep away from windows and stay low to the ground to avoid detection.
e) Close your office blinds or other window treatment.
f) Turn off lights and computer monitors.





g) Do not use cell phones as doing so may give your location away – turn off ringers.
h) Remain in the washroom, if you are already there.
i) Remain quiet and do not enter hallways.
j) If in a hallway, seek shelter in the nearest room, office or designated safe room.
k) Should the fire alarm sound, do not evacuate the building unless one:
   - has firsthand knowledge that there is a fire in the building, or
   - has been advised by a Floor Emergency Officer or first responders (e.g. Police/Security) to evacuate the building.
l) Stay put until police give the "all clear".
m) Follow police instructions and be available to provide statement.

### 3.2 Duties of the Building Emergency Organization (BEO)

#### 3.2.1 Duties of the Responsible Building Authority (RBA)

a) Make certain local authorities have been notified;
b) Advise the Chief Building Emergency Officer (CBEO) to proceed with the lockdown procedures;
c) When possible, advise the personnel and visitors by intercom, voice communication or other readily available means of the reason and need to lockdown;
d) Maintain communication with the CBEO to exchange reports and vital information on the state of the emergency;
e) Co-ordinate action with other involved parties such as the CBEO, Building Owner, the local police authority and other tenants of the building;
f) Ensure that the Border Operations Center (BOC) is advised by phone at or by email.

#### 3.2.2 Duties of the Chief Building Emergency Officer (CBEO) and Deputy Chief Building Emergency Officer (DCBEO)

a) Implement lockdown procedures as advised by local emergency responders and RBA;
b) Advise the Regional or HQ Security Officer who in turn will contact the Security and Professional Standards Directorate (SPSD) at Headquarters;
c) Take steps to ensure no one leaves their respective areas (if required);
d) Advise the Floor Emergency Officers (FEOs) to lock office and external doors and close windows and window treatments.
e) Advise employees to refrain from using personal cellphones and to follow instructions;
f) Assist the RBA as required.

#### 3.2.3 Duties of the Floor Emergency Officers (FEO)

a) Assist the RBA and the CBEO/DCBEO;
b) Await and follow instructions from the CBEO;
c) Report to the CBEO any problems encountered.



# Planification de l'intervention en cas d'urgence dans les immeubles
## Annexe L : Confinement barricadé

### 1. Introduction

Un confinement barricadé doit seulement être utilisé en cas d'incident violent grave ou de menace de violence **à l'intérieur** de l'immeuble, ou en lien avec celui-ci. Dans une telle situation, les employés doivent cesser de travailler et se réunir dans une salle qui peut être verrouillée de l'intérieur et attendre d'autres directives des principaux représentants de l'immeuble ou des responsables de l'exécution de la loi.

### 2. Communication

Si on découvre une situation pouvant exiger un confinement barricadé, il faut suivre la procédure de communication suivante :

- la personne qui fait la découverte doit communiquer immédiatement avec le **911** si elle peut le faire en toute sécurité;
- si possible, communiquer avec un gestionnaire, un agent de sécurité régional ou de l'Administration centrale (AC) ou un agent de secours d'étage sur place, et fournir le plus de renseignements possible;
- habituellement, un confinement barricadé d'urgence est annoncé dans un premier temps par interphone, communication vocale ou tout autre moyen facilement accessible;
- les alarmes d'évacuation incendie ne sont pas déclenchées;
- une fois alertées concernant l'application d'un confinement barricadé, les personnes doivent être informées de ne pas utiliser leurs téléphones cellulaires personnels. De plus, elles doivent suivre toutes les directives données par l'agent de sécurité ministériel (ASM), la direction, l'agent de sécurité régional ou de l'AC, ou encore l'agent de secours d'étage sur place;
- tout renseignement accessible doit être rapidement communiqué par l'ASM, l'agent de secours en chef de l'immeuble, son adjoint ou un remplaçant de l'agent de sécurité régional ou de l'AC, et les autorités policières locales.

### 3. Rôles et responsabilités

#### 3.1 Tâches des employés

Dans le cadre d'une procédure de confinement barricadé, les occupants doivent être informés de prendre les mesures suivantes :

a) composer le 911 et, si c'est possible de le faire en toute sécurité, informer un gestionnaire ou la sécurité;
b) **NE PAS** actionner l'alarme incendie;

c) se verrouiller immédiatement dans leur bureau ou la pièce la plus proche. Si la pièce ne peut pas être verrouillée, barricader la porte à l'aide de meubles. Si la pièce ne comporte pas de porte, se cacher sous un bureau ou de façon à ne pas être vu;
d) se déplacer dans un coin sécuritaire pour réduire la visibilité — rester loin des fenêtres et rester près du sol pour éviter d'être vu;
e) fermer les stores ou les autres garnitures de fenêtre du bureau;
f) éteindre les lumières et les écrans d'ordinateur;
g) ne pas utiliser les téléphones cellulaires puisque cela pourrait permettre de les localiser — éteindre les sonneries;
h) rester dans les toilettes, s'ils sont déjà là;
i) rester silencieux et ne pas pénétrer dans les corridors;
j) s'ils se trouvent dans un corridor, trouver un abri dans la pièce, le bureau ou la salle de sécurité désignée le plus proche;
k) si l'alarme incendie est activée, ne pas évacuer l'immeuble, sauf dans les cas suivants :
   - ils savent par eux-mêmes qu'il y a un incendie dans l'immeuble;
   - l'agent de secours d'étage ou les premiers intervenants (p. ex. police/sécurité) leur disent d'évacuer l'immeuble;
l) ne pas bouger jusqu'à ce que la police signale la fin de l'alerte;
m) suivre les directives des policiers et être disponibles pour fournir une déclaration.

### 3.2 Tâches de l'organisme des secours de l'immeuble (OSI)

#### 3.2.1 Tâches de l'autorité responsable de l'immeuble (ARI)

a) S'assurer que les autorités locales ont été informées.
b) Demander à l'agent de secours en chef de l'immeuble (ASCI) d'appliquer la procédure de confinement barricadé.
c) Si possible, informer le personnel et les visiteurs par interphone, communication vocale ou un autre moyen facilement accessible des motifs du confinement barricadé et du besoin de le faire.
d) Maintenir la communication avec l'ASCI pour échanger des comptes rendus et des renseignements essentiels sur l'état de la situation d'urgence.
e) Coordonner la prise de mesures avec les autres parties touchées, comme l'ASCI, le propriétaire de l'immeuble, les policiers et les autres locataires de l'immeuble.
f) S'assurer que le Centre des opérations frontalières (COF) est informé par téléphone, au                    , ou par courriel.

#### 3.2.2 Tâches du chef des services de secours de l'immeuble (CSSI) et du chef adjoint des services de secours de l'immeuble (CASSI)

a) Appliquer la procédure de confinement barricadé à la demande des intervenants d'urgence locaux et de l'ARI.
b) Informer l'agent de sécurité régional ou de l'AC, qui, quant à lui, communiquera avec la Direction de la sécurité et des normes professionnelles (DSNP), à l'Administration centrale.
c) Prendre les mesures nécessaires pour s'assurer que personne ne quitte sa zone respective (au besoin).
d) Informer les agents de secours d'étages (ASE) de verrouiller les portes des bureaux et les portes donnant sur l'extérieur et de fermer les fenêtres et les garnitures de fenêtre.

e) Informer les employés qu'ils ne doivent pas utiliser leurs téléphones cellulaires personnels et qu'ils doivent suivre les directives.
f) Aider l'ARI, au besoin.

**3.2.3 Tâches des agents de secours d'étage (ASE)**

a) Aider l'ARI et le CSSI/son adjoint.
b) Attendre et suivre les directives du CSSI.
c) Communiquer au CSSI tout problème rencontré.



# Building Emergency Response Planning
## Appendix M: Shelter-in-Place Procedures

### 1. Introduction

*A* shelter-in-place should be used when it is desirable to secure the building due to an ongoing situation **outside** and not related to the building: whether it is a criminal activity, such as a bank robbery nearby, or an environmental or weather related situation such as a chemical spill or extreme weather conditions. In this situation, the exterior doors are locked to discourage occupants from leaving and possibly getting in harm's way. Occupants are asked to remain where they are until further instructions are provided.

### 2. Communication

If a situation possibly requiring a shelter-in-place is discovered, the following communication procedures should be followed:

- The individual making the discovery should immediately contact a manager, a Regional or Headquarters (HQ) Security Officer, or an on-site Floor Emergency Officer and provide as much information as possible;
- An emergency shelter-in-place will usually be first announced by intercom, voice communication or other readily available means;
- Fire evacuation alarms are **not** to be sounded;
- Once alerted as to a shelter-in-place, individuals should be advised to refrain from using personal cellphones and should follow any instructions issued by the Departmental Security Officer (DSO), management, a Regional or HQ Security Officer, or the on-site Floor Emergency Officer; and
- Available information should be quickly communicated by the DSO, Chief Building Emergency Officer, Deputy Chief Building Emergency Officer or alternate to the Regional or HQ Security Officer and local police authorities.

### 3. Roles and Responsibilities

#### 3.1 Duties of Employees

As part of shelter-in-place procedures, occupants should be informed to undertake the following actions:

a) Close blinds or other window treatments.
b) Stay away from the windows.
c) Stay in your work area and await further instructions.
d) Provide for the safety of clients or visitors by asking them to stay, not leave.
e) Procedures will vary depending on the reason for the shelter-in place – wait for instructions.





- Employees may be allowed to move freely within the building
- Employees may be allowed to continue normal activities.

f) You may be asked by the DSO or Building Emergency Organization (BEO) to move to lockdown if the threat is headed toward your building.

g) Employees must wait for instructions from the DSO or BEO before evacuating or leaving the building.

### 3.2 Duties of the Building Emergency Organization (BEO)

#### 3.2.1 Duties of the Responsible Building Authority (RBA)

a) Make certain local authorities have been notified (if required);
b) Advise the Chief Building Emergency Officer (CBEO) to proceed with the shelter-in-place procedures;
c) When possible, advise the personnel and visitors by intercom, voice communication or other readily available means of the reason and need to shelter-in-place;
d) Maintain communication with the CBEO to exchange reports and vital information on the state of the emergency;
e) Co-ordinate action with other involved parties such as the CBEO, Building Owner, the local police authority and other tenants of the building;
f) Ensure that the Border Operations Center (BOC) is advised by phone at or by email.

#### 3.2.2 Duties of the Chief Building Emergency Officer (CBEO) and Deputy Chief Building Emergency Officer (DCBEO)

a) Implement shelter-in-place procedures as advised by local emergency responders and RBA;
b) Advise Regional or HQ Security Officer who in turn will contact the Security and Professional Standards Directorate (SPSD) at Headquarters;
c) Take steps to ensure no one leaves their respective areas (if required);
d) Advise the Floor Emergency Officers (FEOs) to lock external doors and close windows and window treatments.
e) Advise employees to refrain from using personal cellphones and to follow instructions;
f) Assist the RBA as required.

#### 3.2.3 Duties of the Floor Emergency Officers (FEO)

a) Assist the RBA and the CBEO;
b) Await and follow instructions from the CBEO;
c) Report to the CBEO any problems encountered.



# Planification de l'intervention en cas d'urgence dans les immeubles

## Annexe M : S'abriter sur place

### 1. Introduction

Il faut utiliser une procédure d'abri sur place lorsqu'il faut sécuriser l'immeuble en raison d'une situation en cours **à l'extérieur** qui n'est pas liée à l'immeuble : que ce soit une activité criminelle, comme un vol de banque tout près, ou une situation environnementale ou météorologique, comme un déversement de produits chimiques ou des conditions météorologiques extrêmes. Dans de telles situations, les portes extérieures sont verrouillées pour décourager les occupants de sortir et de s'exposer à des dangers. On demande aux occupants de rester là où ils sont jusqu'à nouvel ordre.

### 2. Communication

Si on découvre une situation pouvant exiger une procédure d'abri sur place, il faut suivre la procédure de communication suivante :

- la personne qui fait la découverte doit communiquer immédiatement avec un gestionnaire, un agent de sécurité régional ou de l'Administration centrale (AC) ou un agent de secours d'étage sur place, et fournir le plus de renseignements possible;
- habituellement, une mesure d'abri sur place d'urgence est annoncée dans un premier temps par interphone, communication vocale ou tout autre moyen facilement accessible;
- les alarmes d'évacuation incendie ne sont pas déclenchées;
- une fois averties qu'elles doivent s'abriter sur place, les personnes doivent être informées de ne pas utiliser leurs téléphones cellulaires personnels. De plus, elles doivent suivre toutes les directives données par l'agent de sécurité ministériel (ASM), la direction, un agent de sécurité régional ou de l'AC ou un agent de secours d'étage sur place;
- tout renseignement accessible doit être rapidement communiqué par l'ASM, l'agent de secours en chef de l'immeuble, son adjoint ou un remplaçant de l'agent de sécurité régional ou de l'AC et les autorités policières locales.

### 3. Rôles et responsabilités

#### 3.1 Tâches des employés

Dans le cadre de la procédure d'abri sur place, les occupants doivent être informés de prendre les mesures suivantes :

a) fermer les stores et les autres garnitures de fenêtre;
b) rester loin des fenêtres;

c) rester dans leur aire de travail et attendre de plus amples directives;
d) assurer la sécurité des clients ou des visiteurs en leur demandant de rester et de ne pas partir;
e) la procédure varie selon la raison pour laquelle il faut s'abriter sur place — attendre des directives;
   - on peut permettre aux employés de continuer à se déplacer librement dans l'immeuble;
   - on peut permettre aux employés de poursuivre leurs activités normales :
f) l'ASM ou l'organisme des secours de l'immeuble (OSI) peuvent vous demander de procéder à un confinement barricadé si la menace se dirige vers votre immeuble;
g) les employés doivent attendre les directives de l'ASM ou de l'OSI avant toute évacuation ou avant de sortir de l'immeuble.

**3.2 Tâches de l'organisme des secours de l'immeuble (OSI)**

**3.2.1 Tâches de l'autorité responsable de l'immeuble (ARI)**

a) S'assurer que les autorités locales ont été informées (au besoin);
b) Demander à l'agent de secours en chef de l'immeuble (ASCI) d'appliquer la procédure d'abri sur place.
c) Si possible, informer le personnel et les visiteurs par interphone, communication vocale ou un autre moyen facilement accessible de la raison pour laquelle il faut s'abriter sur place et du besoin de le faire;
d) Maintenir la communication avec l'ASCI pour échanger des comptes rendus et des renseignements essentiels sur l'état de la situation d'urgence;
e) Coordonner la prise de mesures avec les autres parties touchées, comme l'ASCI, le propriétaire de l'immeuble, les autorités policières locales et les autres locataires de l'immeuble;
f) S'assurer que le Centre des opérations frontalières (COF) est informé par téléphone, au ou par courriel.

**3.2.2 Tâches du chef des services de secours de l'immeuble (CSSI) et du chef adjoint des services de secours de l'immeuble (CASSI)**

a) Appliquer la procédure d'abri sur place à la demande des intervenants d'urgence locaux et de l'ARI;
b) Informer l'agent de sécurité régional ou de l'Administration centrale, qui, quant à lui, communiquera avec la Direction de la sécurité et des normes professionnelles (DSNP), à l'Administration centrale;
c) Prendre les mesures nécessaires pour s'assurer que personne ne quitte sa zone respective (au besoin);
d) Informer les agents de secours d'étages (ASE) de verrouiller les portes extérieures et de fermer les fenêtres et les garnitures de fenêtre;
e) Informer les employés qu'ils ne doivent pas utiliser leurs téléphones cellulaires personnels et qu'ils doivent suivre les directives;
f) Aider l'ARI, au besoin.

**3.2.3Tâches des agents de secours d'étage (ASE)**

a) Aider l'ARI et le CSSI;
b) Attendre et suivre les directives du CSSI;
c) Communiquer au CSSI tout problème rencontré.

Canada Border Services Agency | Agence des services frontaliers du Canada



# Building Emergency Response Planning
## Appendix N: Active Shooter Procedure

**This procedure applies to all non-operational CBSA office space and should be read in conjunction with the:**

- *Emergency and Essential Information* page on Atlas under the *"Health, Safety and Security"* main menu tab;
- *Guideline in the Event of a Critical Injury or Death of an Employee in the Line of* Duty, and;
- *Critical Incident Stress Management (CISM) Guidelines and Standard Operating Procedures.*

In the case of armed CBSA officers trained in the use of force, the responses dictated by their training, the procedure in the *Arming Policy Suite*, and the applicable *Regional Critical Incident Management Plan,* developed in accordance with the *Emergency Preparedness, All Hazards Approach* will take precedence.

### 1. Introduction

An Active Shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims.

Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of police officers is required to stop the shooting and mitigate harm to victims. Because active shooter situations are often over within 10 to 15 minutes, before police officers arrive on the scene and engage, individuals must be prepared both mentally and physically to deal with an active shooter situation.

### 2. Security of CBSA Facilities

In all CBSA facilities physical security safeguards are applied based on the threat environment of each facility. These safeguards include access control measures such as the presence of security guards, identification cards and building pass procedures, layers of protection such as security zones, perimeter controls such as fencing surrounding properties, security cameras, etc. These safeguards play a primarily preventative role by deterring an adversary from passing into Agency controlled areas, detecting suspicious or unauthorized activities, allowing appropriate response, and undertaking recovery operations.

In each facility occupied by the CBSA, there is an emergency response plan aligned with the requirements of the *Occupational Health and Safety Regulations Part XVII*, and the *Treasury Board's Standard for fire safety planning and fire emergency organization* that includes:

- An Emergency Evacuation Plan that comprises procedures for the safe evacuation of a building and/or facility; and
- Based on a risk analysis, procedures for all possible emergency situations at a building and/or facility, such as fires, bomb threats, hostage takings, earthquakes, chemical or environmental accidents, etc.





## 3. How to respond to an active shooter

Quickly determine the most reasonable way to protect your own life. Remember that visitors and clients are likely to follow the lead of employees and managers during an active shooter situation.

### 3.1 Run

If there is an accessible and safe escape path, attempt to evacuate the premises.
Be sure to:

- Have an escape route and plan in mind;
- Evacuate regardless of whether others agree to follow;
- Leave your belongings behind;
- Help others escape, if possible;
- Advise other individuals from entering an area where the active shooter may be;
- Call 911 when you are safe.

### 3.2 Hide

If the active shooter is nearby:

- If you are in a hallway, get into a room, stay there and secure the door;
- Silence your cell phone and/or any other electronic device;
- Turn off any source of noise (i.e., radios, televisions);
- Hide behind large items (i.e., cabinets, desks);
- Remain quiet.

If evacuation and hiding out are not possible:

- Remain calm;
- Dial 911, if possible, to alert police to the active shooter's location;
- If you cannot speak, leave the line open and allow the dispatcher to listen.

### 3.3 Fight

If the shooter is at close range and you cannot hide or escape – **and this is a decision only you can make** – fighting back may be your best chance for survival. To do so you need to disrupt or incapacitate (take out) the shooter by:

- Acting as aggressively as possible towards him/her;
- Throwing any object and improvising weapons;
- Yelling; and
- Committing to your actions.

## 4. Police Response

The police intervention aims to stop the active shooter as soon as possible. Police officers will proceed directly to the area in which the last shots were heard.

- Police officers usually arrive in teams of four (4);
- Police officers may wear regular patrol uniforms, plain clothes or external bulletproof vests, helmets, and other tactical equipment;
- Police officers may be armed with rifles, shotguns, handguns;
- Police officers may use pepper spray or tear gas to control the situation;
- Police officers may shout commands, and may push individuals to the ground for their safety.

**5. How to Respond When Police Officers Arrive on Scene**

- Remain calm, and follow police officers' instructions;
- Put down any items in your hands (i.e., bags, jackets);
- Immediately raise hands and spread fingers;
- Keep hands visible at all times;
- Avoid making quick movements toward officers such as holding on to them for safety;
- Avoid pointing, screaming and/or yelling;
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which police officers are entering the premises.

**6. Information to Provide to Police Officers or 911 Operators**

- Location of the active shooter(s);
- Number of shooters, if more than one;
- Physical description of shooter(s);
- Number and type of weapons held by the shooter(s);
- Number of potential victims at the location;
- Movements of the active shooter(s) if possible.

Note that the first police officers to arrive at the scene will not stop to help injured persons. Expect rescue teams comprised of additional police officers and emergency medical personnel to follow the initial officers. These rescue teams will treat and remove any injured persons. They may also call upon able-bodied individuals to assist in removing the wounded from the premises.

**7. Safe Location**

Once you have reached a safe location or an assembly point, you will likely be held in that area by police until the situation is under control, and all witnesses have been identified and questioned. It is important that you avoid discussing the incident with other witnesses in order to prevent statement contamination.
Do not leave until authorities have instructed you to do so.



# Planification d'urgence pour les immeubles
## Annexe N : Procédure en cas de tireur actif

**La présente procédure s'applique à tous les bureaux de l'ASFC non opérationnel et doit être lue en parallèle avec ce qui suit :**

- la page _Renseignements essentiels et d'urgence_ dans Atlas, sous l'onglet « *Santé et sécurité* » du menu principal;
- les _Lignes directrices à suivre dans le cas d'une blessure grave ou du décès d'un employé dans l'exercice de ses fonctions_;
- les _Lignes directrices et procédures normales en cas de gestion du stress dû à un incident critique (GSIC)_.

Dans le cas des agents armés de l'ASFC ayant reçu une formation sur le recours à la force, les interventions dictées par leur formation, la procédure de la _Suite de la politique d'armement_ et le *plan régional de gestion des incidents critiques* qui s'applique, élaboré en conformité avec le document _Mesures d'urgence, une approche globale_, auront préséance.

### 1. Introduction

Un tireur actif est une personne qui s'acharne activement à tuer ou qui tente d'assassiner d'autres personnes dans un lieu restreint où se trouvent beaucoup de gens; dans la plupart des cas, les tireurs actifs utilisent une ou des armes à feu, et la sélection de leurs victimes ne repose sur aucun plan ou méthode particulière.

Les situations mettant en scène un tireur actif sont imprévisibles et se transforment rapidement. Habituellement, le déploiement immédiat des agents de police est nécessaire pour faire cesser la fusillade et réduire les blessures que pourraient subir les victimes. Étant donné que les situations mettant en scène un tireur actif ne durent jamais plus de 10 à 15 minutes, avant que les agents de police arrivent sur les lieux et interviennent, les personnes doivent être prêtes, mentalement et physiquement, à faire face à un tireur actif.

### 2. Sécurité des installations de l'ASFC

Dans toutes les installations de l'ASFC, des mesures de protection liées à la sécurité physique sont prises en fonction du contexte de menace de chaque installation. Ces mesures de protection incluent des mesures d'accès contrôlé, comme la présence de gardiens de sécurité, des procédures misant sur des cartes d'identité et des laissez-passer, des couches de protection, comme des zones de sécurité, des contrôles périmétriques, tels que des clôtures qui entourent les propriétés, des caméras de sécurité, etc. Ces mesures de protection jouent principalement un rôle préventif et visent à dissuader un ennemi d'entrer dans les zones contrôlées de l'Agence, et à détecter des activités suspectes ou interdites, à permettre une intervention appropriée et à entreprendre des activités de rétablissement.





Dans chaque installation occupée par l'ASFC, il y a un plan d'intervention d'urgence harmonisé avec les exigences de la partie XVII du *Règlement canadien sur la santé et la sécurité au travail* et la *Norme pour le plan d'évacuation d'urgence et l'organisation des secours en cas d'incendie* du Conseil du Trésor, qui inclut :

- un plan d'évacuation d'urgence comprenant des procédures d'évacuation sécuritaires d'un immeuble ou d'une installation;
- à la lumière d'une évaluation des risques, des procédures liées à toutes les situations d'urgence possibles dans un immeuble ou une installation, comme un incendie, une menace à la bombe, la prise d'otages, un tremblement de terre, des accidents chimiques ou environnementaux, etc.

**3. Comment réagir à un tireur actif**

Déterminer rapidement la façon la plus raisonnable de vous protéger. N'oubliez pas que les clients et les visiteurs suivront probablement l'exemple des employés et des gestionnaires s'il y a un tireur actif.

**3.1 Courir**

S'il y a une voie d'évacuation accessible et sécuritaire, tentez d'évacuer les lieux.
Assurez-vous de faire ce qui suit :

- ayez un trajet et un plan d'évacuation en tête;
- évacuez les lieux, peu importe si les autres acceptent de suivre ou non;
- n'apportez pas vos effets personnels;
- aidez les autres à évacuer les lieux, si possible;
- conseiller les autres individus d'entrer dans un endroit où pourrait se trouver un tireur actif;
- composez le 911 lorsque vous serez en sécurité.

**3.2 Se cacher**

Si un tireur actif est près de vous :

- si vous êtes dans un corridor, entrez dans une pièce, restez-y et verrouillez la porte;
- mettez votre téléphone cellulaire ou vos autres appareils électroniques en mode silencieux;
- éteignez toute source de bruit (p. ex. radio et télévision);
- cachez-vous derrière de gros meubles (p. ex. classeurs et bureaux);
- restez tranquille.

Si vous ne pouvez ni évacuer les lieux ni vous cacher :

- restez calme;
- composez le 911, si possible, pour avertir la police de l'endroit où se trouve le tireur actif;
- si vous ne pouvez pas parler, laissez la communication ouverte afin de permettre au répartiteur des services d'urgence d'écouter.

**3.3 Lutte**

Si le tireur est tout près et que vous ne pouvez ni vous cacher ni fuir — **et c'est une décision que seul vous pouvez prendre** —, l'attaquer est peut-être votre meilleure chance de survie. Pour y arriver, vous devez déranger le tireur ou le neutraliser (l'éliminer) en faisant ce suit :

- soyez le plus agressif possible à son égard;
- lancez des objets et des armes improvisées;
- criez;
- donnez tout ce que vous avez.

**4. Intervention policière**

L'intervention policière vise à arrêter le tireur actif le plus rapidement possible. Les agents de police se rendront directement à l'endroit où les derniers coups de feu ont été entendus.

- Les agents de police arrivent habituellement en équipes de quatre (4).
- Les agents de police peuvent porter leur uniforme régulier, une tenue civile ou des gilets pare-balles, des casques et d'autres équipements tactiques;
- Les agents de police peuvent être armés de carabines, de fusils ou d'armes de poing.
- Les agents de police peuvent utiliser du gaz poivré ou du gaz lacrymogène pour contrôler la situation.
- Les agents de police peuvent crier des ordres et pousser des gens au sol pour assurer leur sécurité.

**5. Comment réagir lorsque des agents de police arrivent sur place**

- Restez calme et suivez les instructions des agents de police.
- Déposez tout objet que vous avez à la main (c.-à-d. sacs, vestons).
- Levez immédiatement les mains en l'air et écartez vos doigts.
- Gardez vos mains visibles en tout temps;
- Évitez de faire des mouvements brusques en direction des agents (p. ex. se cramponner à eux pour votre sécurité).
- Évitez de pointer et de crier.
- N'arrêtez pas pour demander de l'aide ou des instructions aux agents; dirigez-vous seulement dans la direction par où les agents sont arrivés.

**6. Renseignements à fournir aux agents de police ou aux répartiteurs du 911**

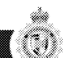
- Lieu où se trouve le(s) tireur(s) actif(s).
- Nombre de tireurs, s'il y en a plus d'un.
- Description physique du ou des tireurs.
- Nombre et types d'armes utilisées par le ou les tireurs.
- Nombre de victimes possibles dans le lieu.
- Déplacements du ou des tireurs actifs, si possible.

Il convient de signaler que les premiers agents de police arrivés sur les lieux n'arrêteront pas pour aider les personnes blessées. Attendez-vous à ce que des équipes de secours composées d'autres agents de police et de personnel médical d'urgence suivent les premiers agents. Ces équipes de secours s'occuperont des personnes blessées et les sortiront de là. Les agents peuvent aussi demander aux personnes qui sont aptes à le faire de les aider à retirer les blessés des lieux.

**7. Lieu sûr**

Une fois que vous vous trouvez dans un endroit sûr ou un lieu de rassemblement, les policiers vous y maintiendront probablement jusqu'à ce que la situation soit sous contrôle et que tous les témoins aient été identifiés et interrogés. Il est important pour vous d'éviter de discuter de l'incident avec d'autres témoins afin de prévenir toute contamination des déclarations.
Ne partez pas avant que les autorités vous aient ordonné de le faire.

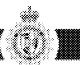
Agence des services frontaliers du Canada | Canada Border Services Agency



# Gestion de la continuité des activités

PROTECTION • SERVICE • INTÉGRITÉ

Canada



## 1. Préambule

Conformément à l'alinéa 6(2)c) de la Loi sur la gestion des urgences (LGU), l'ASFC est tenue de préparer des plans et de prendre des dispositions pour assurer la prestation continue des services ou des produits essentiels durant une interruption de service.

## 2. Date d'entrée en vigueur

La présente politique entre en vigueur en octobre 2012.

Elle remplace la Politique de planification de la continuité des activités en date du 7-05-2009.

## 3. Application

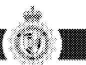
La présente politique s'applique à tous les employés de l'ASFC (permanents, temporaires, occasionnels et à temps partiel), aux employés contractuels et au personnel des organismes privés, ainsi qu'aux personnes détachées ou affectées à l'ASFC, y compris les étudiants.

## 4. Contexte

La gestion de la continuité des activités (GCA) est un processus de gestion proactif qui permet d'assurer la prestation des services ou la production des produits essentiels durant une interruption de service.

Les activités de gestion de la continuité des opérations consistent notamment à :

- déterminer, évaluer, analyser et prioriser l'environnement essentiel d'une organisation (services de base, services de soutien, infrastructure de gestion de l'information et des technologies de l'information (GI-TI), biens et dépendances).
- planifier, mesurer et prendre des dispositions pour assurer la prestation continue des services et produits essentiels qui faciliteront la reprise des activités habituelles d'une organisation.
- définir les ressources nécessaires pour assurer la continuité des activités, telles que le personnel, les renseignements, le matériel, les affectations financières, les conseils juridiques, la protection des infrastructures et les locaux.
- mettre en œuvre un processus rigoureux d'amélioration des capacités pour s'assurer que tous les aspects des plans et des ententes sont continuellement mis à l'essai et appliqués, que les leçons tirées sont intégrées et que l'information est systématiquement mise à jour.



## 5. Définitions

### Biens

Les biens tangibles ou intangibles du gouvernement du Canada, notamment, à titre indicatif mais non exhaustif, l'information sous toutes ses formes et les supports, les réseaux, les systèmes, le matériel, les biens immobiliers, les ressources financières, la confiance des employés, la confiance du public et la réputation du gouvernement à l'échelle internationale.

### Service essentiel

Un service qui, s'il faisait défaut, causerait un préjudice important à la santé, à la sécurité ou au bien-être économique des Canadiens ou au fonctionnement efficient du gouvernement du Canada.

### Dépendance

Les services de fournisseurs internes/externes, les biens et les ressources utilisés pour assurer le service essentiel.

### Interruption de service

Une panne ou un arrêt des opérations qui ne fait pas partie des activités habituelles de l'organisation, et qui peut avoir une incidence sur les services ou entraîner leur arrêt et, dans certains cas, entraîner une catastrophe.

## 6. Autorisations

La présente politique est établie en vertu de l'alinéa 6(2)c) de la Loi sur la gestion des urgences (2007, c.15) et de la Politique sur la sécurité du gouvernement.

## 7. Énoncé de politique

L'ASFC est chargée d'établir, de mettre en œuvre et d'entretenir un programme de gestion de la continuité des activités (PGCA) afin d'assurer la prestation continue de ses services et biens essentiels qui contribuent à la santé, à la sécurité et au bien-être économique des Canadiens, ainsi qu'au fonctionnement efficace du gouvernement.

### 7.1 Objectif stratégique



La présente politique a pour objectif de s'assurer que la gestion de la continuité des activités est appliquée dans l'ensemble de l'ASFC afin de permettre la coordination efficace de la prestation des services essentiels en cas d'interruption de service.

**7.2 Résultats prévus**

Les résultats prévus de la présente politique sont les suivants :

- les services de l'Agence seront évalués et analysés;
- des plans et des dispositions seront établis pour les services considérés essentiels;
- les plans, les processus et les procédures seront mis à l'essai et appliqués;
- la capacité de l'Agence de continuer d'assurer la prestation de ses services de base durant une interruption de service sera sans cesse renforcée;
- les plans seront conservés et mis à jour en temps opportun.

**8. Exigences**

Les **gestionnaires** sont chargés de déterminer la criticité du(des) service(s) dont ils assurent la prestation.

Les **gestionnaires des services** essentiels sont chargés d'élaborer, de mettre en œuvre, de mettre à l'essai et de tenir à jour des plans et des dispositions pour assurer la prestation continue des services essentiels.

Les **employés de l'ASFC** sont responsables de prendre connaissance de leurs rôles et de leurs responsabilités figurant dans les plans (le cas échéant).

**8.1 Exigences en matière de surveillance et de rapports**

La Direction de la sécurité et des normes professionnelles (DSNP) examinera périodiquement la présente politique. Afin d'appuyer le processus d'examen, la DSNP est chargée de définir et d'entreprendre toutes les activités de surveillance et d'évaluation destinées à déterminer si les objectifs de la politique demeurent pertinents et atteignables et si les exigences sont respectées.

Les exigences en matière d'établissement de rapports seront saisies par l'entremise de recommandations découlant des exercices réguliers et des vérifications (internes et externes) et seront communiquées chaque année au président et(ou) au premier vice-président.

**9. Conséquences**







L'inobservation de la présente politique et de ses directives à l'appui peut avoir diverses conséquences, notamment que l'ASFC ne soit pas en mesure d'atténuer les menaces et de continuer à assurer la prestation des services essentiels. En substance, ne pas suivre la politique peut rendre l'Agence vulnérable et incapable de remplir son mandat imposé par la loi.

**10. Rôles et responsabilités**

**Président et premier vice-président**

- S'assurer que l'on a mis en œuvre un programme de gestion de la continuité des activités nécessaire pour gérer la continuité des activités de l'ASFC;
- assurer le leadership stratégique de l'Agence durant les interruptions de service;
- communiquer avec les intervenants internes et externes et les consulter afin de renforcer la capacité de gestion de la continuité des activités de l'Agence et d'appuyer les mesures prises par le gouvernement du Canada à ce chapitre.

**Responsable de la sécurité de l'Agence (RSA)**

Par l'entremise du Programme de gestion des urgences et de la continuité des activités, le responsable de la sécurité de l'Agence est chargé de :

- élaborer et tenir à jour une série de politiques, de procédures, d'outils et de produits de communication et de sensibilisation afin d'appuyer la mise en œuvre de la politique de gestion de la continuité des activités dans l'ensemble de l'Agence;
- tenir à jour un inventaire des services essentiels de l'ASFC;
- examiner et surveiller l'élaboration, l'application et l'entretien du plan de continuité;
- s'assurer que des stratégies, des plans et une structure de régie sont en place pour assurer la prestation continue des services essentiels de l'Agence;
- coordonner, avec l'avis de la Direction générale de l'information, des sciences et de la technologie (DGIST) et de la Direction générale des opérations, les éléments clés du programme, tels que l'entraînement et la formation afin de s'assurer de l'état de préparation de l'Agence;
- fournir du soutien et des conseils aux intervenants de l'Agence pour l'application et la mise en œuvre du processus de GCA;



- élaborer et dispenser la formation sur la GCA;
- s'assurer que les résultats des activités et des mesures de GCA sont, au besoin, communiqués aux niveaux hiérarchiques pertinents de l'Agence;
- coordonner l'information relative aux mesures de gestion de la continuité durant une urgence.

**Vice-président, Direction générale des opérations**

- Assurer en temps opportun la réalisation des activités de GCA pour la Direction générale des opérations, qui comprend tous les bureaux d'entrée (BE) et les secteurs opérationnels des régions;
- s'assurer que le Centre des opérations frontalières (COF) fonctionne au point de coordination durant une interruption de service ayant une incidence sur les services essentiels, et informer le responsable de la sécurité de l'Agence (RSA) lorsqu'un plan de continuité des activités est activé;
- assurer la communication avec les partenaires internes et externes (étrangers, nationaux, provinciaux et locaux) et la consultation de ces derniers afin de renforcer la capacité de l'Agence à maintenir la prestation des services essentiels dont la Direction générale des opérations est responsable durant une interruption de service.

**Vice-président, Direction générale de l'information, des sciences et de la technologie (DGIST)**

- S'assurer en temps opportun de la réalisation des activités de GCA pour la DGIST;
- établir des stratégies de continuité des activités de TI de l'ASFC;
- appuyer les activités de GCA en recueillant, analysant et établissant les priorités des besoins en matière de TI de chaque direction générale, des bureaux d'entrée et des secteurs opérationnels;
- élaborer des normes, des lignes directrices, des modèles, des processus et des outils pour l'Agence;
- s'assurer que des plans complets de continuité des activités de TI (y compris des plans de reprise après un sinistre) sont élaborés, mis en œuvre, mis à l'essai et tenus à jour pour l'ASFC;
- élaborer et dispenser une formation sur la continuité des activités de TI;
- assurer la communication avec les partenaires internes et externes (étrangers, nationaux, provinciaux et locaux) et la consultation de ces derniers afin de renforcer la capacité de l'Agence à poursuivre la prestation des services essentiels dont la Direction générale de l'information, des sciences et de la technologie est responsable durant une interruption de service.



### Autres vice-présidents

- S'assurer de la réalisation en temps opportun des activités de GCA de leurs directions générales respectives;
- assurer la communication avec les partenaires internes et externes (étrangers, nationaux, provinciaux et locaux) et la consultation de ces derniers afin de renforcer la capacité de l'Agence à poursuivre la prestation des services essentiels de leur direction générale durant une interruption de service.

### Gestionnaires des services essentiels

- Définir et établir le niveau de criticité du(des) service(s) essentiel(s) qu'ils assurent;
- définir les biens essentiels et leurs dépendances pour le(s) service(s) essentiel(s);
- élaborer, exercer et tenir à jour des plans et des ententes pour leur(s) service(s) essentiel(s);
- activer, au besoin, leur(s) plan(s) et informer en conséquence le Centre des opérations frontalières (COF), et transmettre en temps opportun des mises à jour;
- désactiver leur(s) plan(s) lors du retour à la normale des activités et rédiger des rapports de suivi.

### Coordonnateurs de la gestion de la continuité des activités

- Coordonner l'élaboration et la mise en œuvre des activités de GCA au sein de leur direction générale et(ou) de leur région;
- fournir une orientation et communiquer les outils liés au recueil des renseignements aux gestionnaires;
- fournir des rapports d'étape réguliers au responsable de la sécurité de l'Agence (RSA);
- représenter la direction générale et(ou) la région aux réunions du Groupe de travail des coordonnateurs de la continuité des activités.

### 11. Références

Les documents de référence suivants s'appliquent à la présente politique :

- Loi sur la gestion des urgences (L.C. 2007, ch.15)



- Politique sur la sécurité du gouvernement
- Norme de sécurité opérationnelle – Programme de planification de la continuité des activités (PCA)

**11.1 Politiques et publications portant sur le sujet**

- Politique de l'ASFC sur la gestion des urgences
- Guide de réalisation d'une analyse des répercussions sur les activités (ARA)
- Guide d'élaboration d'un plan de continuité des activités (PCA)
- Lignes directrices pour les exercices des plans de continuité des activités
- Cycle d'entretien d'un plan de continuité des activités (PCA)
- Norme opérationnelle de sécurité sur l'identification et la catégorisation des biens
- Politique sur la sécurité de la gestion de l'information et des technologies de l'information (GI-TI)
- Politique fédérale en matière de gestion des urgences (Sécurité publique)

**12. Demandes de renseignements**

Pour de plus amples renseignements, veuillez communiquer avec :

CBSA-ASFC, Security Policy-Politiques sur la Securite
410, avenue Laurier Ouest, 10e étage
Ottawa, Ontario, K1A 0L8

Canada Border Services Agency | Agence des services frontaliers du Canada



# Policy on Business Continuity Management

PROTECTION • SERVICE • INTEGRITY





## 1. Preamble

In accordance with the Emergency Management Act (EMA), Subsection 6(2)(C), the CBSA is responsible for preparing plans and arrangements to ensure the continued delivery of critical services or products during a service disruption.

## 2. Effective Date

This policy takes effect in October 2012.

It replaces the Business Continuity Planning Policy dated 2009-05-07.

## 3. Application

This policy is applicable to all CBSA employees (permanent, term, casual, and part-time), contract and private agency personnel and to individuals seconded or assigned to CBSA, including students.

## 4. Context

Business Continuity Management (BCM) is a proactive management process that ensures critical services or products are delivered during a service disruption.

BCM activities include:

Identifying, assessing, analyzing and prioritizing the organizations' critical environment (services, support services, IM-IT infrastructure, assets and dependencies).

Planning, measuring and making arrangements to ensure the continuous delivery of critical services and products which facilitate the organizations ability to return to business as usual.

Identifying necessary resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodations.

A rigorous capability improvement process to ensure all aspects of the plans and arrangements are continuously tested and exercised, lessons learned are incorporated and the information is systematically updated.

## 5. Definitions

### Assets







Tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, system, material, real property, financial resources, employee trust, public confidence and international reputation.

**Critical Service**

It is a service which if unavailable would result in a high degree of injury to the health, safety and security or economic well-being of Canadian or to the efficient functioning of the Government of Canada.

**Dependency**

The reliance of a critical service on internal/external service provider, assets and/or resources.

**Service Disruption**

An outage event which is not part of a standard operating business which may impact or interrupt services and, in some cases, may lead to disaster.



## 6. Authorities

This policy is issued under the Emergency Management Act (2007, c.15) Subsection 6(2) (C) and the Policy on Government Security.

## 7. Policy Statement

The CBSA is required to develop, implement and maintain a Business Continuity Management Program (BCMP) to provide for the continued availability of its critical services and assets that contribute to the health, safety, security and economic well-being of Canadians, and the effective functioning of government.

### 7.1 Policy Objective

The objective of this policy is to ensure that BCM is applied throughout the CBSA to achieve effective coordination for the continued availability of critical services in the event of a service interruption.

### 7.2 Expected Results

The expected results of this policy are:

the Agency's services will be assessed and analyzed;

plans and arrangements will be developed for services identified as critical;







plans, processes and procedures will be tested and exercised;

the Agency's capability to continue its core services during a service interruption will be continuously improved; and

plans will be maintained and updated in a timely fashion.

**8. Policy Requirements**

**Managers** are responsible for determining the criticality of the service(s) they deliver.

**Critical Service Managers** are responsible for developing, implementing, exercising and maintaining plans and arrangements to ensure the continuous delivery of their critical service(s).

**CBSA Employees** are responsible for familiarizing themselves with their roles and responsibilities within the plans (if applicable).

**8.1 Monitoring and Reporting Requirements**

The Security and Professional Standards Directorate (SPSD) will periodically review this policy. To support the review process, the SPSD is responsible for identifying and undertaking any monitoring and assessment activities to determine whether the policy's objective remains relevant and achievable and whether its requirements are being adhered to.

Reporting requirements are captured through recommendations resulting from regular exercises and audits (internal and external) and will be reported to the President and/or the Executive Vice-President on an annual basis.

**9. Consequences**

Consequences of non-compliance with this policy and its supporting guidelines may contribute to the CBSA being unable to mitigate threats and continue to offer critical services. In essence, not following the BCM policy may render the Agency vulnerable and unable to meet its legislated mandate.



**10. Roles and Responsibilities**

**President/Executive Vice-President**

Ensures the implementation of a Business Continuity Management Program responsible for the management of continuity activities for the CBSA;

Provides Agency strategic leadership during service interruptions; and







Communicates and consults with internal and external stakeholders to strengthen Agency continuity management capacity and support Government of Canada continuity efforts.

**Departmental Security Officer (DSO)**

Through the Emergency and Business Continuity Management Program, the DSO:

Develops and maintains a suite of policies, procedures, tools and communication and awareness products to support the implementation of the BCM policy throughout the Agency;

Maintains an inventory of CBSA critical services;

Reviews and monitors continuity plan development, exercising and maintenance;

Ensures strategies, plans and governance are in place to support continuous service delivery of the Agency's critical services;

Coordinates, with input from ISTB and Operations Branches, key program components such as exercising and training to ensure Agency readiness;

Provides support and guidance to Agency stakeholders in the application and implementation of the BCM process;

Develops and delivers BCM training;

Ensures that the results of BCM activities and efforts are communicated to the appropriate Agency levels as required;

Coordinates information related to continuity management efforts during an emergency.

**Vice-President Operations Branch**

Ensures the timely completion of the BCM activities for the Operations Branch which includes all the Ports of Entry (POE) and operational areas in the regions;

Coordinates, with input from ISTB and the Security and Professional Standards Directorate (SPSD), key program components such as exercising and training to ensure Agency readiness;

Ensures the Border Operations Centre (BOC) operates as point of coordination during a service disruption impacting critical services and notifies the DSO when a business continuity plan is activated; and

Ensures communication and consultation with internal and external partners (international, national, provincial and local) to strengthen the Agency's ability to continue delivering its operational critical services during a service disruption.







## Vice-President Information Science and Technology Branch (ISTB)

Establishes the CBSA IT Continuity strategies;

Supports the BCM activities by gathering, analyzing and prioritizing the IT requirements of each Branch, POE and operational area;

Coordinates, with input from Operations Branch and the Security and Professional Standards Directorate (SPSD), key program components such as exercising and training to ensure Agency readiness;

Develops IT Continuity standards, guidelines, models, processes and tools for the Agency;

Ensures comprehensive IT Continuity Plans (including Disaster Recover Plans) are developed, implemented, tested and maintained for the CBSA;

Develops and delivers IT Continuity training; and

Ensures communication and consultation with internal and external partners (international, national, provincial and local) to strengthen the Agency's ability to continue delivering its IT critical services during a service disruption.



## Other Vice-Presidents

Ensures the timely completion of the BCM activities for their respective branches; and

Ensures communication and consultation with internal and external partners (international, national, provincial and local) to strengthen the Agency's ability to continue delivering their branches critical services during a service disruption.

## Critical Services Managers

Identify and establish the criticality of their CBSA critical service(s);

Identify the critical assets and dependencies for their critical service(s);

Develop, exercise and maintain plans and arrangements for their critical service(s);

Activate their plan(s) when required and advises the BOC accordingly and provides timely status updates; and

Deactivate their plan(s) when business returns to normal and completes the follow up reports.

## Business Continuity Management Coordinators







Coordinate the development and implementation of the BCM activities within their branch and/or region;

Provide guidance and share tools related to the gathering of information with the managers;

Provide ongoing status reports to the DSO; and

Represent the branch and/or region at business continuity coordinators working group.

**11. References**

The following reference material is applicable to this policy:

Emergency Management Act (2007, c.15)

Policy on Government Security

Operational Security Standard – Business Continuity Planning (BCP) Program

**11.1 Related Policies and Publications**

CBSA Emergency Management Policy

Guide to Completing the Business Impact Analysis (BIA)

Guide to Completing the Business Continuity Plan (BCP)

Guideline to Exercising Business Continuity Plans

The BCP Maintenance Cycle

The Security Operational Standard for the Identification of Assets

IT/IM Policy on Security

Public Safety's Emergency Management Policy

**12. Enquiries**

For more information, please contact:

CBSA-ASFC, Security_Policy-Politiques_sur_la_Securite
410 Laurier Avenue West, 10th Floor
Ottawa, Ontario, K1A 0L8







# Policy on Abuse, Threats, Stalking and Assaults against Employees

**Purpose**

1. The Canada Border Service Agency (CBSA) is committed to protecting, supporting and assisting its employees and their families where there has been any act of abuse, threat, stalking and assault directed against them or their property in the performance of their duties, or as a direct result of their employment.

**Effective Date**

2. This policy takes effect on March 1, 2015.

**Policy Objective**

3. The objective of this policy is to ensure the physical and mental well-being of employees and their families who have been the subject of verbal or written abuse; written or verbal threats; stalking and assaults that occur while the employees are performing their duties or when they are not performing their duties, but as a direct result of their employment with the CBSA. It also provides an outline of the procedures to be followed by employees and managers when these situations occur.

**Application**

4. This policy applies to all employees (permanent, term, casual, part-time) of the CBSA, contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students. Family members of the aforementioned are included in the application of this policy.

**Definitions**

5. Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

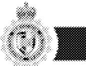
**Policy Requirements**

6. Employees must:

- Report all cases of abuse, threats, stalking and assaults to their manager, at the earliest opportunity;
- Report all cases of abuse, threats, stalking and assaults to the police;
- Report all cases of verbal abuse to their manager, at the earliest opportunity, unless the employee feels that the incident was inconsequential or not worth reporting;
- Report all cases of clients requesting the completion of questionnaires or forms, or any other actions which are purposely intended to hinder the employee from performing their duties;
- Make complete notes as soon as possible after the incident has taken place;







- Request the guidance and assistance of their managers if they are required to call on or otherwise deal with a known difficult or violent client;
- Request police intervention, if warranted; and
- Cooperate with the police and/or the Court once a complaint is made.

Note:

In extreme cases personal protection may be sought by employees and/or their families from the police. This must be done through their manager.

7. Managers must take all necessary and reasonable steps to prevent and/or protect employees against potential or further injury or damage by:

- Ensuring that all cases of abuse, threats, stalking and assaults are reported to the police;
- Ensuring that all employees are made aware of this policy;
- Providing their employees with information/awareness sessions and guidance on how to deal with threatening situations;
- Designating an employee to take names, addresses and statements from witnesses when the police have not done so;
- Cooperating with the Regional or Headquarters Security Office and police on the provision of protection for the employee and/or the employee's family when warranted;
- Coordinating with the police and other available resource services, such as the Employee Assistance Program (EAP), when dealing with the physical, mental or emotional well-being of employees and family members, as required;
- Reporting all cases of abuse, threats, stalking and assaults to their Director, the Security and Professional Standards Directorate (SPSD), and the Regional or Headquarters Security Office;
- Ensuring that records are maintained of all reported incidents. These records are usually reported to and maintained by the Regional or Headquarters Security Office;
- Ensuring that follow-ups on the status of pending charges are conducted;
- Ensuring that employees are apprised of any progress regarding complaints; and
- Involving the workplace Health and Safety Committee in any significant incidents.

**Monitoring and Reporting Requirements**

8. The Security and Professional Standards Directorate will monitor compliance with this policy.










**References:**

9. The following references apply to this policy:

CBSA Code of Conduct
EN Manual Part 6 Chap. 5 Sec 58 – Use of Force
Security Volume, Standard for Security Incident Reporting
*Canada Labour Code, Part II*

**Enquiries**

For more information, please contact:

Security and Professional Standards Directorate
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca





Agence des services frontaliers du Canada | Canada Border Services Agency



# Politique sur les mauvais traitements, menaces, poursuites et voies de fait à l'égard des employés

**Objet**

1. L'Agence des services frontaliers du Canada (ASFC) s'engage à protéger, à soutenir et à aider ses employés ainsi que les membres de leur famille contre tout mauvais traitements, menaces, poursuites et voies de fait commis contre eux ou contre leurs biens dans l'exercice de leurs fonctions, ou qui découlent directement de ces fonctions.

**Entrée en vigueur**

2. Cette politique entre en vigueur le 1er mars 2015.

**Objectif de la politique**

3. Cette politique a pour objet de veiller au bien-être physique et mental des employés et des membres de leur famille qui ont été victimes de mauvais traitements verbaux ou écrits, de menaces verbales, écrites ou physiques, ou de poursuites et de voies de fait, qui surviennent pendant que les employés exercent leurs fonctions ou en tout autre temps lorsque l'incident découle directement des fonctions exercées par les employés pour le compte de l'ASFC. On y trouve également un aperçu des procédures que les employés et les gestionnaires doivent suivre lorsque de telles circonstances surviennent.

**Application**

4. La présente politique s'applique à tous les employés de l'ASFC (permanents, nommés pour une période déterminée, occasionnels et à temps partiel), au personnel à contrat et au personnel d'agences privées, ainsi qu'aux personnes en détachement ou en affectation à l'ASFC, y compris les étudiants. Cette politique s'applique aux membres de la famille des personnes susmentionnées.

**Définitions**

5. Des définitions précises provenant de sources qui font autorité se trouvent dans le Lexique de la terminologie en sécurité.

**Exigences de la politique**

6. Les employés doivent :

- porter à l'attention de leur gestionnaire tout cas de menaces, de poursuites et de voies de fait et ce, le plus tôt possible;
- signaler tous les cas de menaces, de poursuites et de voies de fait à la police;







- signaler tous les cas de violence verbale à leur gestionnaire le plus tôt possible, sauf s'ils considèrent que l'incident ne porte pas à conséquence et qu'il ne vaut pas la peine d'en faire état;
- signaler tous les cas de clients qui demandent que soient remplis des questionnaires ou des formulaires, ou toute autre mesure visant expressément à empêcher l'employé d'exercer ses fonctions;
- consigner par écrit les détails de l'incident le plus rapidement possible après que cet incident se soit produit;
- demander des conseils et de l'aide à leur gestionnaire s'ils sont tenus de rencontrer un client reconnu pour être difficile ou violent, ou s'ils sont appelés à traiter avec lui de quelque manière que ce soit;
- demander l'intervention de la police au besoin ; et ;
- collaborer avec la Cour et la police lorsqu'une plainte a été déposée

Note :

- Dans des cas extrêmes, une demande de protection personnelle peut être demandée à la police par les employés et/ ou par leurs familles. Cette demande doit être présentée par l'entremise de leur gestionnaire;

7. Les gestionnaires doivent prendre toutes les mesures raisonnables nécessaires suivantes afin de prévenir d'autres blessures ou dommages qui pourraient être infligés aux employés :

- veiller à ce que tous les cas de mauvais traitements, menaces, poursuites et voies de fait soient signalés à la police;
- veiller à ce que tous les employés soient mis au courant de la présente politique;
- présenter aux employés des séances d'information ou de sensibilisation et des conseils concernant la façon de se comporter dans des situations de menaces;
- désigner un employé pour consigner les noms, adresses et exposés des témoins lorsque ce n'est pas fait par la police;
- coopérer avec les bureaux régionaux de la sécurité ou avec la Sécurité à l'AC et la police au sujet de la protection à fournir à un employé et (ou) aux membres de sa famille lorsqu'une telle demande est faite;
- coopérer avec la police et d'autres ressources disponibles, telles que le Programme d'aide aux employés (PAE), pour assurer le bien-être physique, mental ou émotionnel des employés et des membres de leur famille au besoin;
- rédiger un rapport sur tous les cas de mauvais traitements, menaces, poursuites et voies de fait et le présenter à leur directeur, à la Direction de la sécurité et des normes professionnelles (DSNP), et au bureau régional de la sécurité ou au bureau de la sécurité de l'Administration centrale;
- s'assurer que tous les incidents signalés sont consignés aux dossiers. Ces dossiers sont généralement tenus par le bureau régional de la sécurité ou au bureau de la sécurité de l'Administration centrale;
- veiller à ce que l'on fasse un suivi approprié des accusations en suspens; veiller à ce que les employés soient informés des progrès accomplis relativement au traitement des plaintes;
- faire participer le Comité de la sécurité et de la santé au travail à tout incident important.










**Processus de responsabilisation**

8. La Direction de la sécurité et des normes professionnelles s'assurera de l'observation de cette politique.

**Références**

9. Les références suivantes s'appliquent à cette politique :

Code de conduite de l'ASFC
Manuel de l'exécution, partie 6, chapitre 5, section 58 – Recours à la force
Volume de sécurité, Signalement des incidents de sécurité
*Code canadien du travail*, partie II

**Demandes de renseignements**

Pour de plus amples renseignements, veuillez communiquer avec la :

Direction de la sécurité et des normes professionnelles
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca





Canada Border Services Agency / Agence des services frontaliers du Canada



# Guidelines for Abuse, Threats, Stalking and Assaults against Employees

These guidelines take effect on March 1, 2015.

This guide is to be read in conjunction with the Policy on Abuse, Threats, Stalking and Assaults against Employees. It applies to employees (and their families) who are subjected to threatening situations involving members of the public (e.g. travellers, clients, etc.). Issues involving internal acts of violence are covered by the Policy on Violence Prevention in the Work Place.

1. The Canada Border Services Agency (CBSA) is committed to protecting, supporting and assisting its employees and their families where there has been any act of abuse, threat, stalking and/or assault directed against them or their property in the performance of their duties or as a direct result of the performance of their duties.

2. Employees of the CBSA may have contact with the public at the workplace, at the client's home or place of business, or any other location, as required by the nature of the duties. It is possible for employees to encounter threatening situations while at the workplace or while performing assigned duties, as a result of the conduct of individuals or groups who may dispute legitimate enforcement actions. In addressing this possibility, the CBSA has developed a policy concerning acts of abuse, threats, stalking, assaults, and property damage directed against employees and their families.

3. In any difficult or dangerous situations, the safety of the employee must be the first priority. Employees must remove themselves from any threatening situation. Employees must protect themselves at all times, ensuring their own safety and that of their families, as well as the safety of their fellow employees and clients. Incidents must be reported to the manager or the Regional or Headquarters Security Office, or to the Security and Professional Standards Directorate (SPSD) at Headquarters.

4. The following guidelines are only intended as basic directions on how to react when confronted with threatening situations although in some instances the word "must" is used to reflect the intent of the Policy. Employees are expected to use sound judgment when dealing with threatening situations and to deal with them or to attempt, when possible, to remove themselves. If, in the everyday performance of their duties, there is a potential for such incidents, it is strongly recommended that information sessions in subjects related to situation diffusion and communication be undertaken.

## For Employees

### Guidelines on How to Handle Abusive or Threatening Incidents

5. Employees are obligated to identify themselves with the appropriate CBSA identification. Employees are also required to explain the reason for, the nature of and the legal authority for the enforcement action.





6. Whenever possible during the conduct of their duties, employees must use their best judgment to identify threats, to prevent threats from occurring and to get assistance and/or maintain lawful purpose without subjecting themselves to the risk of assault or abuse.

7. In the event that an on-going situation with a client turns abusive or threatening, the meeting, interview, or telephone call is to be terminated as quickly as possible.

**Reporting of incidents**

8. All incidents resulting in abuse, threats, stalking and/or assaults, regardless of their origin or nature, must be reported to the manager who will in turn inform the appropriate Director and their Regional or Headquarters Security Office. All incidents of abuse, threats, stalking and/or assaults reported by employees to managers must be reported to the local police. In urgent situations, employees may contact the police directly and subsequently report the incident to their manager.

9. Such occurrences constitute security incidents and are to be reported as required by the CBSA Security Volume.

10. Cases of verbal abuse should be reported by employees to their managers at the earliest opportunity, unless the employees feel that the verbal abuse is non-consequential or not worth reporting. When employees report verbal abuse, these cases must be reported as any other security incident.

11. In all cases, meticulous notes should be made as soon as reasonably practical containing as much detail as possible regarding the incident, the words spoken, etc. which will aid in the subsequent investigation and/or legal proceedings.

**Other considerations**

12. After an incident the employee must prepare a detailed report and provide a copy to the appropriate manager. The employee will cooperate with police, the Court, security representative(s) and/or the workplace Health and Safety Committee, when inquiries are conducted.

13. Employees must alert their manager, when they notice any situation which could put employees at risk, for example, a client who may have hostile intentions and displays a weapon; is suspected or believed to be impaired by drugs or alcohol and demonstrates belligerent behaviour; threatens an employee with physical harm; makes a bomb threat; or threatens the institution with other property damage.

**What information to give to police**

14. Information that employees or managers may give to police following incidents of abuse, threats, stalking and/or assaults should be limited to details describing the individual/client and the circumstances, in particular, the individual's/client's name, where the incident occurred, and the facts showing how the threat impacts the employee and the Agency. The individual's current home or business address, if different from where the incident occurred and the individual's date of birth may be provided only if specifically required by the police.

15. Employees and managers must not provide the police with specifics of the dealings between the CBSA and the individual/client, such as how much the client owes or the nature of the enforcement action since this would constitute a breach of confidentiality. Although discretion must be exercised, sufficient information must be provided as to not hinder a police investigation.

16. Employees are expected to cooperate with the police or the Court as witnesses during any subsequent investigations or legal proceedings.

**Specific Guidelines**

**Telephone Abuse**

17. While speaking with clients on the telephone, employees may be subjected to name-calling, swearing, or ridicule, directed either at them or at the organization. While this behaviour by clients is considered rude or disrespectful, it is not usually threatening. The client may have poor communication skills, or be frustrated, impatient or angry.

18. Employees who receive rude or disrespectful telephone calls from clients, at the office or at home, should try to calm the individual and attempt to identify the caller. Clients calling off-duty employees on their private residential lines are to be directed to call the employee's business number during working hours. All such calls are to be reported as security incidents.

19. Employees should attempt to isolate the client's specific irritants that created the situation and to confine the conversation to that subject. This can be achieved by asking questions to clarify any ambiguities or obtain facts, remaining objective and polite and avoiding objectionable behaviour. Should the abuse continue, the employee is to warn the caller that such behaviour will not be tolerated and that the telephone call will be terminated. If the offensive behaviour continues the employee is to calmly end the conversation, record what transpired and promptly forward the report to their immediate manager and the Regional or Headquarters Security Office.

20. If the same client continues to be verbally abusive in subsequent telephone calls, or continues to call the employee at his/her private residence after a request by the employee to stop, the employee must report to the manager and consider other options, such as:

- Having management contact the client to try to obtain voluntary compliance;
- Preparing a letter, for the Director's signature, outlining the problem and requesting the client to discontinue the abusive behaviour (the letter must be sent using registered mail to support future legal action);
- Conducting any further business only through correspondence;
- Inviting the client to the office and meeting with the client in the presence of another CBSA employee;
- Requesting the manager assume responsibility for the file and deal with the client;
- Requiring that the records be made available at a CBSA office; and
- Requesting legal advice should the client refuse to comply with the requested action.

**Telephone Threats**

21. Abusive telephone calls become *threatening* calls when a client states or expresses an intention to punish, harm or injure an employee or family member, to damage private or CBSA property, or to infringe on the employee's rights with a view to limiting the employee's freedom of action. All such threats are to be reported to the manager and to the Regional or Headquarters Security Office.

22. Employees who receive a threatening telephone call at home from a client should try to identify the caller and obtain as much detailed information as possible. Such details should include the caller's identity, the reason behind the threat, and exact wording, if possible. If another person is present, the employee should ask that person to listen in on a telephone extension. Furthermore, the employee will advise the manager at the earliest opportunity, unless it appears to the employee that the threat is imminent, in which case the employee should contact the police directly and then advise the manager.

23. Employees who receive a threatening telephone call at the office should try to keep the individual talking and, if possible, have a manager or another employee listen in to confirm the threat. Employees may suggest that the caller speak with the manager to try to resolve and defuse the situation. The employee or the manager should explain to the caller the serious nature of the threat. The police must be contacted.

24. In cases of telephone threats, the employee should use all available means to identify the caller.

*** Note:** The manager should contact the local telephone company to verify if call trace is possible and to determine what specific procedures are required in order to trace a caller. Discuss the steps to follow with local police as they can also provide support for a call trace warrant.

**Threatening correspondence**

25. If an employee receives threatening correspondence, at the office or at home, the employee is to avoid unnecessary handling of the correspondence to avoid contaminating any evidence which may be lifted from the correspondence itself or its packaging. The items should be placed in a plastic bag and turned over to the manager or the Regional or Headquarters Security Office as soon as possible. If the threat is received by electronic transmission, social media or e-mail, contact the Regional or Headquarters Security Office or information technology administrator for assistance to ensure that evidence is preserved. They, as well as the local police, can provide further details on Chain of Custody / Evidence handling procedures to ensure continuity and court admissibility. These items have evidentiary value and will be given to the police for investigation.

**Offensive or threatening interviews on or outside CBSA premises**

26. Employees should be aware that any interview or meeting, on-site or off-site, could become threatening, even though there is no indication of the possibility at the outset. It is recommended that before entering a situation where they think or suspect there is potential for an incident involving threats or violence, employees should advise their manager of their concerns.

27. Managers who are made aware of concerns by employees should consider the following avenues:

- Cancel the meeting or interview;
- Re-schedule the meeting so it is held on CBSA premises and attend the meeting with the employee or assign a colleague of the employee to be present at the meeting;
- Request that the client produce records at a CBSA office.

28. If, during a meeting on CBSA premises, the client's language or behaviour becomes offensive or causes the employee to feel that the business purposes of the meeting cannot be carried out, or cause the employee to feel threatened, the employee should terminate the meeting as soon as possible, and advise the manager of the incident. If the employee experiences any kind of difficulty in the meeting room or in trying to leave the room, the employee should set off any available alarm system, or attract the attention of other employees. Where there is significant indication that this might occur, the employee should not conduct the meeting/interview

unless accompanied and should choose a suitable interview room for the purpose equipped with a tested duress/panic alarm.

29. Employees experiencing threats during meetings held off-site must terminate the meeting as soon as possible and advise the manager of the incident. If the employee experiences any kind of difficulty leaving the meeting, the employee should try to attract the attention of other persons in the vicinity and call 911.

**Client hindering employee duties / Assault**

30. In situations where the client attempts to hinder or interfere with employees performing their duties, the client is to be advised that the CBSA will act fairly, decisively and firmly, and in accordance with the law to ensure that the examination, questioning, audit, investigation or other business transaction is completed.

31. Remember that the safety of the employee is paramount and must prevail above and beyond any action and takes precedence over any duty. The employee may be the last line of defence and will have no choice than to react to protect himself/herself, colleagues or the public.

32. Any employee who is assaulted on or off a CBSA site must withdraw from the danger area if he or she feels that his/her life is in danger to a location from where the employee could attract the attention of other employees or of the general public. In the case of Border Services Officers, they may be able to contain the risk by using defensive equipment and/or use of force training. The employee should also use any available alarm system to attract attention.

33. Any employee who is prevented from leaving the danger area should seek help from nearby persons, by shouting or by setting off any available alarm system. Best judgment should be exercised if such a situation occurs when an employee is working in isolation.

34. Any employee who has been assaulted should get a medical examination as soon as possible after the incident.

35. The employee should call the police as soon as possible. Otherwise, upon being informed of the incident, the manager must call the police.

36. Abuse, threats, stalking and assaults are Security Incidents and must be reported as stipulated in the CBSA Security Volume.

**Stalking**

37. Once an employee suspects that someone is following them, the first consideration must be personal safety. This is best assured by proceeding to a public location from where it would be easier to attract the attention of others and call the police.

38. Stalking is considered a criminal offence under the Criminal Code of Canada and must therefore be reported to the police, as soon as possible. Details on the person's appearance and behaviour should be recorded as soon as is feasible after the incident to provide an accurate description of the event. The employee must also report the incident to the manager at the earliest opportunity.

39. Managers will arrange for personal protection from the police if circumstances warrant, based on a threat and risk assessment and if the employee so wishes. In the interim local police may increase local surveillance

and start a formal investigation while the employee's manager seeks legal support to impose court legal actions (e.g. restraining order, arrest, etc.).

40. Employees will need to cooperate with the police and the Court once a complaint is made.

**Visible weapons**

41. Any employee who notices a person in a CBSA facility, who is carrying what is or appears to be a weapon, shall immediately call 911 and subsequently report the incident to the Regional or Headquarters Security Office or a manager. The employee must not attempt to apprehend the person. CBSA Border Services Officers are to follow the directives in the Use of Force Policy.

42. Employees required to visit client premises, especially in rural areas, must be aware that clients may own firearms or other weapons. An employee who perceives a risk or is threatened with a weapon must leave the premises immediately, call the police if the threat is imminent and report the incident to their manager or the Regional or Headquarters Security Office.

43. In the event of an incident involving weapons, robbery attempts, bomb threats, etc. immediately initiate the measures as per the Security Volume – Building Emergency Planning procedures.

**Guard dogs**

44. In any situation where employees are confronted with guard dogs or other animals, they should request that the owner restrain and remove the animal from the meeting place. If the owner refuses to restrain or remove the animal, the meeting must be terminated. It can be construed as an assault if the owner orders the animal to attack the employee.

45. Employees are to advise their manager of all incidents in this category. The employees may also request police presence if necessary at this or at any subsequent meeting or make other arrangements.

## For Managers

**Immediate action**

46. The first priority for a manager at the scene of an incident of abuse, threats, stalking or assaults, is to take any appropriate action required to protect the employees and family members and to prevent further injury or damage. Such actions may include calling emergency services such as the police and/or an ambulance.

**Reporting and investigating**

47. The CBSA has a duty to provide its employees with a safe working environment. Therefore, all cases of abuse, threats, stalking and assaults must be reported to the police with or without the employee's consent, as the threat may impact on the safety of other employees and their families.

48. As soon as possible after an incident, the manager must notify the director and the Regional or Headquarters Security Office. The manager will also advise any other person specified by local administrative procedures.

49. Where, as a result of offensive and threatening situations, an audit or other enforcement action has to be terminated, as discussed in earlier sections, the manager should ensure that enforcement actions are not postponed indefinitely. The manager will consider other actions permitted by law.

50. The manager is responsible for ensuring that an incident report for every occurrence is prepared and forwarded to the Regional or Headquarters Security Office in accordance with the CBSA Security Volume.

51. Where special arrangements, (such as altering travel patterns to and from work, doubling with a co-worker, temporary change of work site, increasing home security protection controls, and in ultimately rare cases moving an employee, etc.) for the protection of an employee have been put in place as a result of an incident, the manager is responsible for periodic re-assessment of the threat to determine if there is a need to continue or increase the security measures in place. Managers are encouraged to contact their Regional or Headquarters Security Office for advice and assistance.

52. The workplace Health and Safety Committee is to be involved in the early stages of any incident involving abuse, threats, a stalking or assault which has been reported by an employee. They will assist in developing and implementing all necessary measures, as well as the review of the trends and development of recommendations for preventive or corrective measures.

## General Information

53. Employees are **NOT** to permit CBSA identification to be photocopied.

54. For reasons of personal security, employees must never provide any personal information such as a home phone number or address, or a driver's license.

**Post-incident help and employee compensation and benefits**

55. It should be noted that CBSA offers support to employees and their family members who have been the target of abuse, threats, stalking and/or assaults. This support is available in many forms, including access to legal services, reimbursement of approved financial costs and/or material damages, counselling and other services. Each case is assessed on its own merit. Local Human Resources advisors should be contacted for details on the support available and for procedures to be followed in order to obtain it.

**Enquiries**

For more information, please contact:
Security and Professional Standards Directorate
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca






# Lignes directrices concernant les mauvais traitements, menaces, poursuites et voies de fait à l'égard des employés

Ces lignes directrices entre en vigueur le 1er mars 2015.

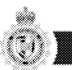
Le présent Guide doit être lu en parallèle avec la Politique sur les mauvais traitements, menaces, poursuites et voies de fait à l'égard des employés. Il s'applique aux employés (et leur famille) soumis à des situations menaçantes mettant en cause le public (c.-à-d. des voyageurs, des clients, etc.). La Politique sur la prévention de la violence en milieu de travail couvre les questions relatives aux actes de violence qui se manifestent à l'interne.

1. L'Agence des services frontaliers du Canada (ASFC) s'engage à défendre, à appuyer et à aider ses employés et les membres de leur famille quand des mauvais traitements, des menaces, des poursuites et des voies de fait sont dirigés contre eux ou leurs biens pendant qu'ils exécutent leurs tâches ou en conséquence directe de l'exécution de leurs tâches.

2. Les employés de l'ASFC peuvent avoir un contact avec le public dans leur bureau ou dans tout autre local de l'ASFC, au domicile ou au lieu d'affaires du client ou en tout autre lieu où ils doivent se rendre en raison de la nature des fonctions à remplir. Il est possible qu'ils aient à faire face à des situations menaçantes quand ils sont au travail ou en raison des fonctions qu'ils ont à remplir, étant donné la conduite de personnes ou de groupes qui contestent peut-être des mesures d'exécution de la loi. L'ASFC a donc élaboré une politique concernant les mauvais traitements, les menaces, les poursuites, les voies de fait et les dommages à la propriété dirigés contre des employés de l'ASFC et leur famille.

3. Dans toute situation dangereuse ou difficile, la sécurité de l'employé doit être la principale priorité. Les employés doivent se tenir à l'écart de toute situation qui présente des risques. Les employés doivent à tout moment penser à leur sécurité et à celle de leur famille ainsi qu'à celle de leurs collègues et de leurs clients. Tout incident doit être signalé au gestionnaire ou au responsable régional de la sécurité ou à l'Administration centrale ou à la Direction de la sécurité et des normes professionnelles (DSNP).

4. Les lignes directrices ci-après ne sont que des orientations de base sur la façon de réagir lorsque l'on est confronté à une situation menaçante même si dans certains cas le mot « devoir » est utilisé afin de refléter le sens de la politique. On s'attend à ce que les employés fassent preuve de jugement pour appliquer les moyens dont ils disposent pour se retirer des situations à risque ou y faire face. Si, dans l'accomplissement de leurs tâches quotidiennes, la possibilité de tels incidents est élevée, il est fortement recommandé qu'ils reçoivent de la formation sur des sujets reliés à la façon de désamorcer une situation conflictuelle et à la communication.



**À l'intention des employés**

**Lignes directrices comment faire face à des incidents marqués par la violence ou représentant une menace**

5. Les employés sont obligés de s'identifier au moyen d'une pièce d'identité appropriée de l'ASFC. De plus les employés doivent indiquer la raison, la nature et le fondement juridique de la mesure d'exécution.

6. Dans la mesure du possible, les employés doivent, lorsqu'ils exercent leurs fonctions, se servir de leur jugement pour déceler les menaces, empêcher qu'elles ne se concrétisent et obtenir de l'aide ou assurer le respect de la loi sans s'exposer à des risques de voies de fait ou de mauvais traitements.

7. Dans l'éventualité où une situation courante de rapport avec un client devient violente ou menaçante, il faut mettre fin à la rencontre, l'entrevue ou à l'appel téléphonique dès que possible.

**Signalement des incidents**

8. Tous les incidents qui donnent lieu à des mauvais traitements, à des menaces, à des poursuites et voies de fait, quelle que soit leur origine ou leur nature, doivent être signalés au gestionnaire qui en informe le directeur compétent et le responsable régional de la sécurité ou à l'Administration centrale. Tous les incidents impliquant des mauvais traitements, des menaces, des poursuites et voies de fait signalés aux gestionnaires par les employés doivent être déclarés à la police locale. Dans les situations d'urgence, les employés peuvent communiquer directement avec la police et faire rapport à leur gestionnaire par la suite.

9. De telles situations constituent des incidents de sécurité et devraient être signalées de la manière indiquée au Volume de sécurité de l'ASFC.

10. Les cas de violence verbale doivent être signalés sans tarder aux gestionnaires, à moins que l'employé considère que l'excès de langage est sans conséquence ou ne mérite pas d'être signalé. Toutefois, les cas de violence verbale déclarés doivent faire l'objet d'un rapport comme tout autre incident de sécurité.

11. Dans tous les cas, des notes méticuleuses doivent être prises aussitôt que possible et doivent contenir le plus de détails possible liés à l'incident – les mots dits, etc. – ce qui sera utile à l'enquête subséquente et / ou lors de procédures judiciaires.

**Autres considérations**

12. Après qu'un incident s'est produit, l'employé doit préparer un rapport détaillé et en fournir copie au gestionnaire concerné. L'employé doit collaborer avec la police, le tribunal, les représentants de la sécurité et le Comité de la sécurité et de la santé au travail lorsque des enquêtes ont lieu.

13. Les employés doivent avertir leur gestionnaire quand ils remarquent une situation susceptible de mettre des collègues en danger, par exemple, un client qui a peut-être des intentions hostiles et qui présente une arme;







qu'on présume ou qu'on croit qu'il a les facultés affaiblies par des drogues ou de l'alcool, qui a un comportement belliqueux ; qui menace de faire subir à un employé des dommages physiques ; ou qui menace de causer des dommages matériels à l'institution.

**Quelle information donner à la police?**

14. L'information que les employés ou les gestionnaires peuvent donner à la police à la suite d'incidents de mauvais traitements, de menaces, de poursuites et voies de fait doivent se limiter aux détails décrivant l'individu/client et les circonstances, en particulier le nom de l'individu, l'endroit où s'est produit l'incident et les faits montrant comment la menace a des répercussions sur l'employé et sur l'Agence. L'adresse actuelle de l'individu à son domicile ou au bureau, si elle est différente de celle où l'incident s'est produit, et sa date de naissance ne peuvent être fournies qu'à la demande expresse de la police.

15. Les employés et les gestionnaires ne doivent pas fournir à la police de détails précis des rapports entre l'ASFC et le client, par exemple, combien le client doit d'argent ou la nature de la mesure d'exécution de la loi, puisque ceci pourrait constituer un manquement à l'obligation de confidentialité. Bien que la discrétion doive être exercée, une quantité suffisante de renseignements doit être fournie de façon à ne pas nuire à l'enquête policière.

16. On s'attend à ce que les employés coopèrent avec la police ou le tribunal en tant que témoins durant toute enquête ou poursuite qui pourrait avoir lieu subséquemment.

**Lignes directrices spéciales**

**Appels téléphoniques injurieux**

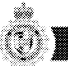
17. Lorsqu'ils parlent à des clients au téléphone, les employés peuvent faire l'objet d'injures, de jurons ou de propos les ridiculisant, ou ridiculisant l'organisation. Bien que ce comportement d'un client soit considéré comme offensant ou irrespectueux, il n'est généralement pas menaçant. Ces clients peuvent avoir de mauvaises techniques de communication ou être frustrés, impatients ou en colère.

18. Les employés qui reçoivent des appels téléphoniques injurieux de la part des clients, au bureau ou à leur domicile, doivent essayer de calmer la personne et tenter de l'identifier. Cela s'applique également aux appels téléphoniques qui deviennent violents. Les clients qui téléphonent à des employés au repos à leur résidence privée doivent être invités à appeler ces employés à leur numéro au bureau, pendant les heures de travail. Tous ces appels doivent être signalés à titre d'incident de sécurité.

19. Les employés doivent également tenter de déterminer les irritants particuliers qui ont donné lieu à la situation et tenter de limiter la conversation à ce sujet. Cela peut se faire en posant des questions pour clarifier toute ambiguïté, en s'enquérant des faits et en demeurant objectif et poli et en évitant tout comportement répréhensible. Si les propos violents se poursuivent, l'employé avertit le client qu'un tel comportement ne peut être toléré et qu'il devra interrompre la communication. Si le comportement offensant continue, l'employé met







fin calmement à l'entrevue, consigne ce qui s'est passé pendant la conversation et envoie rapidement le rapport à son supérieur immédiat et au bureau régional de la sécurité ou à la Sécurité à l'AC.

20. Si, au cours de conversations subséquentes, le même client continue de faire usage de violence verbale ou d'appeler l'employé à sa résidence privée après que celui-ci lui a indiqué de cesser, l'employé doit faire rapport à son gestionnaire et envisager l'une des options suivantes :

- faire communiquer la direction avec le client pour qu'elle tente de l'inciter à observer la loi volontairement;
- rédiger une lettre, pour signature par le directeur, exposant le problème et demandant que le client mette fin au comportement violent (la lettre doit être envoyée par courrier recommandé à l'appui de future action juridique);
- poursuivre toute relation d'affaires ultérieures par la poste;
- inviter le client à venir au bureau et le rencontrer en présence d'un autre employé de l'ASFC;
- demander au gestionnaire de prendre le dossier en charge et de faire affaires directement avec le client;
- demander que le dossier soit mis à la disposition du bureau de l'ASFC;
- demander un avis juridique si le client refuse de se conformer à la mesure demandée.

**Menaces par téléphone**

21. Les appels injurieux deviennent des appels *de menace* lorsqu'un client déclare ou exprime son intention de punir ou de causer du tort ou des blessures à un employé ou aux membres de sa famille, d'endommager la propriété privée ou celle de l'ASFC, ou d'empiéter sur les droits de l'employé avec l'intention de limiter sa liberté d'action. De telles menaces doivent être signalées au gestionnaire et au bureau régional de la sécurité ou à la Sécurité à l'AC.

22. Les employés qui reçoivent un appel téléphonique de menaces de la part d'un client à leur domicile devraient tenter d'identifier la personne qui appelle et d'obtenir des renseignements aussi détaillés que possible. Ces renseignements devraient comprendre l'identité de la personne qui appelle, la raison de son appel et la façon exacte, si possible, dont elle s'est exprimée. Si une autre personne est présente, l'employé devrait lui demander d'écouter sur un poste supplémentaire. De plus, l'employé doit, à la première occasion, informer le gestionnaire à moins qu'il lui semble que la menace soit imminente; dans ce cas, l'employé peut informer la police directement et le faire savoir à son gestionnaire par la suite.

23. Les employés qui reçoivent des appels téléphoniques de menaces au bureau devraient faire en sorte que la conversation se poursuive le plus longtemps possible et, s'ils le peuvent, demander à un gestionnaire ou à un autre employé d'écouter et de confirmer la menace. Ils peuvent aussi proposer à la personne qui appelle de parler avec le gestionnaire en vue de résoudre et de désamorcer la situation. L'employé ou le gestionnaire, selon le cas, doit expliquer à l'appelant qu'un appel de menace est de nature sérieuse. La police doit être informée.







24. Dans les cas où un employé reçoit des menaces par téléphone, il devrait utiliser tous les moyens à sa disposition pour identifier la personne qui appelle.

*** Remarque :** Le gestionnaire doit communiquer avec l'entreprise téléphonique locale afin de vérifier s'il est possible de dépister l'appel et de déterminer quelles procédures particulières sont nécessaires pour dépister la personne ayant fait l'appel. Discuter des étapes à suivre avec la police locale car ils peuvent également fournir un appui pour un mandat afin de tracer l'appel.

**Correspondance contenant des menaces**

25. Si un employé reçoit de la correspondance contenant des menaces, au bureau ou à son domicile, il doit éviter toute manipulation inutile de cet envoi pour éviter de fausser toute preuve qui peut être tirée du message ou de son contenant. Les objets doivent être placés dans un sac de plastique et retournés au gestionnaire ou au bureau régional de la sécurité ou à la Sécurité à l'AC dès que possible. Si de la correspondance contenant des menaces est reçue par voie électronique ou par courriel, il faut communiquer avec le responsable régional de la sécurité ou à l'Administration centrale ou l'administrateur des applications informatiques pour s'assurer que les éléments de preuve sont préservés. Ces objets qui ont une valeur probante seront remis à la police pour enquête.

**Entrevues contenant des propos injurieux ou menaçant sur les lieux de travail ou à l'extérieur de l'ASFC**

26. Les employés devraient être conscients que toute entrevue ou rencontre se déroulant sur les lieux de travail ou à l'extérieur peut donner lieu à des menaces même si cette possibilité ne semble pas exister au premier abord. Par conséquent, il est recommandé qu'avant de s'engager dans une situation dans laquelle ils pensent ou présument qu'il y a une possibilité d'incident impliquant des menaces ou de la violence, les employés devraient en informer leur gestionnaire.

27. Les gestionnaires qui sont mis au courant que leurs employés sont inquiets avant une entrevue devraient envisager l'une ou l'autre des options suivantes :

- annuler la rencontre ou l'entrevue;
- modifier le rendez-vous afin qu'il ait lieu dans les locaux de l'ASFC et assister à la rencontre de l'employé et du client, ou désigner un collègue pour qu'il soit présent durant la rencontre;
- demander au client de produire des documents à un bureau de l'ASFC.

28. Si au cours d'une réunion dans les locaux de l'ASFC, le client utilise un langage injurieux ou à un comportement violent ou fait en sorte que l'employé se sente menacé ou que l'objet de la rencontre ne peut être réalisé, l'employé doit y mettre fin aussi tôt que possible et informer le gestionnaire de l'incident. Si l'employé éprouve une difficulté quelconque dans la pièce où se déroule l'entrevue ou en tentant de sortir de celle-ci, l'employé doit déclencher le système d'alarme ou attirer l'attention des autres employés. Là où il y a forte indication que cela pourrait se produire, l'employé ne doit pas mener la réunion/entrevue sans être accompagné et devrait choisir une salle d'entrevue équipé d'une alarme de panique/testé sous contrainte.







29. Les employés qui sont victimes de menaces au cours de réunions tenues en dehors des locaux doivent y mettre fin dès qu'ils le peuvent et informer le gestionnaire de l'incident. Si l'employé a des difficultés à quitter le lieu de la rencontre, il doit tenter d'attirer l'attention des autres personnes qui se trouvent à proximité et composer le 911.

**Client empêchant des employés d'exercer leurs fonctions/voies de fait**

30. Lorsqu'un client tente d'empêcher les employés d'exercer leurs fonctions ou de les entraver, il doit être informé que l'ASFC prendra des mesures équitables, définitives, fermes et conformes à la loi pour faire en sorte que l'examen, l'interrogatoire, la vérification, l'enquête ou toute autre transaction opérationnelle soit effectué.

31. Il est essentiel de se rappeler que la sécurité des employés est de la plus haute importance et doit avoir priorité sur toute action ou préséance sur l'exécution de toute fonction. L'employé peut être le dernier moyen de défense et n'aura d'autre choix que de réagir pour se protéger, protéger ses collègues ou protéger le public.

32. Tout employé qui subit des voies de fait dans les locaux de l'ASFC ou à l'extérieur doit se retirer de l'endroit considéré comme dangereux et se diriger vers un lieu où il lui est possible d'attirer l'attention des autres employés ou du public en général. Dans le cas des agents des services frontaliers, ils pourraient être en mesure d'atténuer le risque à l'aide de l'équipement de défense ou en ayant recours à la force. L'employé doit également se servir de tout système d'alarme disponible pour attirer l'attention.

33. Tout employé qui est empêché de quitter la zone dangereuse doit chercher à obtenir de l'aide auprès de personnes qui se trouvent à proximité en criant ou en déclenchant un système d'alarme. Il faut être prudent si les voies de fait sont exercées contre un employé travaillant seul ou dans un endroit isolé.

34. Tout employé ayant été dans une situation de voies de fait doit subir un examen médical dès que possible.

35. L'employé doit appeler la police aussi tôt que possible ou le gestionnaire doit le faire dès qu'il est informé de l'incident.

36. Les mauvais traitements, les menaces, les poursuites et les voies de fait sont des incidents de sécurité qui doivent être signalés, tel qu'il est énoncé dans le Volume de sécurité de l'ASFC.

**Poursuites**

37. Lorsqu'un employé soupçonne qu'on le suit, la première considération est d'assurer sa sécurité personnelle. Pour ce faire, l'employé doit se rendre à un endroit public d'où il sera plus facile d'attirer l'attention d'autres personnes et d'appeler la police.

38. Les poursuites sont considérées comme une offense criminelle dans le *Code criminel* et doivent être signalées à la police le plus tôt possible. Des précisions sur l'apparence et le comportement de la personne







doivent être notées le plus rapidement possible après l'incident afin de fournir une description exacte de l'événement. L'employé doit aussi aviser son gestionnaire aussi tôt que possible.

39. Les gestionnaires peuvent demander de l'assistance aux policiers pour la protection personnelle de l'employé si la situation l'indique, en fonction de l'évaluation des menaces et des risques, et si l'employé le souhaite. En attendant, la police locale peut accroître la surveillance et démarrer une enquête officielle pendant que le gestionnaire de l'employé sollicite un soutien juridique pour imposer des actions en justice (ordonnance de non-communication, arrestation, etc.).

40. Les employés doivent collaborer avec la police et le tribunal une fois qu'une plainte est portée.

**Armes visibles**

41. Un employé qui remarque dans les installations de l'ASFC une personne qui transporte ce qui semble être une arme doit immédiatement composé le 911, puis en informer le bureau de la sécurité de la région ou de l'Administration centrale ou un gestionnaire. L'employé ne doit pas essayer d'arrêter la personne lui-même. Les agents des services frontaliers de l'ASFC doivent suivre les directives de la politique sur le recours à la force.

42. Les employés qui doivent se rendre chez des clients, en particulier ceux situés dans des zones rurales, doivent être au courant que ces clients possèdent peut-être des armes à feu ou d'autres armes. L'employé qui perçoit un risque ou que l'on menace avec une arme doit quitter les lieux immédiatement, appeler la police si la menace est imminente et signaler l'incident à son gestionnaire ou au bureau de la sécurité de la région ou de l'Administration centrale.

43. En cas d'incident concernant des armes, des tentatives de vol, des alertes à la bombe, etc., les employés doivent immédiatement suivre les procédures définies dans le Volume de sécurité – Plan d'urgence pour les immeubles.

**Chiens de garde**

44. Lorsque des employés doivent faire face à des chiens de garde ou à d'autres animaux, ils doivent demander au propriétaire de les tenir en laisse et de les faire sortir du lieu de la rencontre. Si le propriétaire refuse de restreindre ou enlever l'animal, la réunion doit être terminée. Elle peut être interprétée comme une attaque si le propriétaire commande l'animal à attaquer l'employé.

45. Les employés qui sont exposés à des incidents de ce type doivent en informer le gestionnaire. Ils peuvent également demander que des policiers soient présents pour toute rencontre subséquente s'ils estiment que cela est nécessaire ou prendre d'autres dispositions.

**À l'intention des gestionnaires**

**Action immédiate**







46. La première mesure à prendre par un gestionnaire sur les lieux d'un incident causant des mauvais traitements, menaces, poursuites ou voies de fait consiste à faire le nécessaire pour protéger l'employé et les membres de sa famille et pour prévenir toute autre blessure ou dommage. Il peut devoir appeler les services d'urgence comme l'ambulance et la police.

**Rapports et enquêtes**

47. L'ASFC est tenue de fournir à ses employés un environnement de travail sécuritaire. Par conséquent, tous les incidents comprenant des mauvais traitements, des menaces, des poursuites et des voies de fait doivent être signalés à la police avec ou sans le consentement de l'employé, étant donné que la menace pourrait avoir des répercussions sur la sécurité d'autres employés et de leur famille.

48. Dès que possible après l'incident, le gestionnaire doit avertir le directeur et le bureau de la sécurité de la région ou de l'Administration centrale. Le gestionnaire doit également aviser toute autre personne mentionnée dans les procédures administratives locales.

49. Lors de toutes situation d'injures et de menaces, il nécessite à prendre les actions nécessaires afin de poursuivre à une vérification ou autre mesure d'exécution, conformément à ce qui a été mentionné dans des sections précédentes. Le gestionnaire doit veiller à ce que les mesures d'exécution ne soient pas remises indéfiniment. Le gestionnaire doit envisager d'autres mesures permises par la loi.

50. Le gestionnaire a la responsabilité de s'assurer qu'un rapport d'incident concernant tout événement soit rédigé et envoyé au bureau de la sécurité de la région ou de l'Administration centrale, conformément au Volume de sécurité de l'ASFC.

51. Lorsque des dispositions spéciales (modifier le trajet entre le travail et le domicile, faire équipe avec un collègue, changer temporairement de lieu de travail, accroître le contrôle de sécurité au domicile, dans de rares cas, réinstaller un employé, etc.) ont été prises pour la protection d'un employé, à la suite d'un incident, le gestionnaire a la responsabilité de réévaluer périodiquement la menace afin de déterminer s'il est nécessaire de maintenir en place les mesures de sécurité prises. Les gestionnaires doivent communiquer avec le bureau de la sécurité de la région ou de l'Administration centrale pour obtenir des conseils et de l'aide.

52. Le Comité de la santé et de la sécurité au travail doit être mis à contribution dès les premières étapes de tout incident comprenant des mauvais traitements, des menaces, des poursuites ou des voies de fait qui a été signalé par un employé afin d'aider à élaborer et à mettre en œuvre les mesures nécessaires, à examiner les tendances et à formuler les recommandations relatives à des mesures préventives ou correctives.

## Renseignements généraux

53. Les employés **ne doivent pas** permettre que les pièces d'identité de l'ASFC soient photocopiées.







54. Pour des raisons de sécurité personnelle, les employés ne doivent jamais fournir des renseignements personnels, tel que numéro de téléphone à la maison, adresse domiciliaire ou permis de conduire.

**Aide, indemnités et dédommagement offerts à l'employé touché après l'incident**

55. Il est à noter que l'ASFC offre du soutien aux employés et à leur famille qui ont été la cible de mauvais traitements, de menaces, de poursuites ou de voies de fait. Ce soutien est offert sous plusieurs formes, notamment Programme d'aide aux employés tel que l'accès aux services juridiques, le remboursement des coûts financiers approuvés ou des dommages matériels, le counseling et d'autres services. Chaque incident est évalué cas-par-cas. On doit communiquer avec les conseillers locaux des Ressources humaines pour obtenir des précisions sur le soutien offert et la procédure à suivre pour l'obtenir.

**Demandes de renseignements**

Pour de plus amples renseignements, veuillez communiquer avec la :
Direction de la sécurité et des normes professionnelles
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca





Mar 13/07

# CBSA Security Manual

# Chapter 27 - Policy - Internal Investigations into Alleged or Suspected Employee Misconduct

## Policy

1. Allegations or suspicions of employee misconduct that includes negligence and carelessness must be promptly reported to the Manager, Internal Affairs and thoroughly investigated.

## Policy Objective

2. The objective of this policy is to ensure that allegations or suspicions of employee misconduct with respect to violations of legislation or other laws, rules and regulations administered by the Canada Border Services Agency (CBSA) are promptly reported and investigated by objective and qualified persons.

## Definitions

3. Misconduct includes any action or inaction by an employee that is contrary to established policy, standards, procedures or practices of the CBSA; violations of legislation for which criminal sanctions are applicable; or violations of other laws, rules and regulations administered by the CBSA or any other act which would bring the CBSA into disrepute or effect the Agency's working relationship with other law enforcement partners.

4. Manager means any person who acts in a supervisory role or managerial capacity.

## Application

5. This policy is applicable to the management of the CBSA, employees (permanent, term, casual, part-time), contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students.

## Policy Requirements

6. Employees are to promptly report to their manager or to Regional Security Officer, or when this is not feasible, to the Corporate Security and Internal Affairs Division (CSIAD), any allegation, suspicion or information concerning employee misconduct.

7. When there is an allegation or suspicion indicating employee misconduct involving violations of criminal legislation or other laws, rules and regulations administered by the CBSA, the Director or the delegated manager must report it immediately to the Manager, Internal Affairs and to the appropriate Vice President. A determination will be made between the local Director and the Manager, Internal Affairs, CSIAD as to who will conduct the investigation.

8. Treasury Board policy stipulates that all suspected cases of loss or theft of money, fraud, or any other offense or illegal act against the Crown by an employee must be fully investigated and reported to the police agency having jurisdiction. Criminal proceedings are generally the exclusive responsibility of law enforcement authorities.

**Responsibilities**

**Internal Affairs Section, Corporate Security and Internal Affairs Division**

9. Internal Affairs, CSIAD, subject to legal and jurisdictional constraints, is responsible for:

- Conducting, or causing to be conducted, investigations into alleged or suspected employee misconduct involving:

  (i.) Theft or loss of revenue, assets, money, seized or abandoned goods;

  (ii.) Unauthorized access to and/or disclosure of client or other sensitive information;

  (iii.) Violations by employees of legislation, or other Federal Statutes (e.g. Customs Act or Immigration Refugee Protection Act or Criminal Code);

  (iv.) Fraudulent transactions on a CBSA system resulting in a reimbursement of reduction of amount owed to which the person or company is not entitled;

  (v.) Fraudulent claims for travel expenses, overtime, leave, relocation, etc.;

  (vi.) Destruction, mutilation, alteration, falsification or concealment of documents, records, certificates, controlled assets or directing, proposing, counseling or causing any persons to take such actions; and

  (vii.) Breaches of the CBSA and Public Service Commission Code of Ethics and Conduct, or other administrative policies.

  (viii.) Other items of serious concern to the CBSA.

- Informing the Vice Presidents of investigations being conducted in their area of responsibility, and reporting the results of the investigation to them and to any other appropriate authorities as required;

- Ensuring that investigations are objective, thorough and conducted by qualified persons, with due respect for the rights and understanding of the obligations of the individuals involved;

- Ensuring that all cases involving the theft of revenue, money, assets, seized or abandoned goods, fraud, destruction, mutilation, falsification or concealment of records or directing,

proposing, counseling or causing any persons to such actions, or any other offenses or illegal acts against the Crown which have been committed by an employee are reported to the police agency having jurisdiction;

- Reporting to management any shortcomings in policies and procedures noted during an investigation, which may have system or organization-wide implications, to allow for corrective measures to be taken to prevent further recurrence of losses and offenses.

**Employees**

10. Employees are expected to obey all legislation and other laws and regulations administered by the CBSA, thereby maintaining their integrity and that of the CBSA.

11. Employees are obliged to provide the necessary cooperation and assistance in the conduct of an investigation. This includes affording complete access to CBSA information systems, documents and records, to the extent that such access is legally permitted.

**Directors or Delegated Managers**

12. Directors or their delegated managers are to report allegations or suspicions of misconduct on the part of employees, in a timely manner, to the Manager, Internal Affairs, CSIAD and to the appropriate Vice President.

13. When it is agreed that local management will conduct the investigation, Directors or their delegated managers are to inform the local Staff Relations consultant and provide a copy of the investigation report, to Internal Affairs, CSIAD and the appropriate Vice President, in a timely manner.

## Reporting Procedures

15. Allegations of employee misconduct may be reported either by telephone or secure facsimile transmission to the Manager, Internal Affairs, and CSIAD, at (613) 948-9347 or by facsimile at (613) 941-6105.

16. These reporting procedures are designed to ensure an effective reporting process and do not detract from the requirement for Vice Presidents to prepare reports, issue sheets, etc. and to advise the President of the CBSA when required.

## Accountability Process

17. The CSIAD will monitor compliance with this policy.

## References

18. The following references are applicable to this policy

- *Financial Administration Act*;
- Public Service Code of Conduct;
- CBSA Conflict of Interest Guidelines;
- Policy on Losses of Money and Offenses and Other Illegal Acts Against the Crown (Treasury Board Manual, Comptrollership Volume, Chapter 4.7);
- CBSA Security Manual, Chapter 15 - Reporting of Security Incidents;
- *Access to Information Act and Privacy Act*;
- *Criminal Code of Canada*;
- *Immigration Refugee Protection Act*
- *Customs Act*
- *Canadian Charter of Rights and Freedoms*;
- Manager's Guide to Conducting Internal Investigations

**Enquiries**

For more information, please contact:

Corporate Security and Internal Affairs Division
9th Floor
410 Laurier Ave
Ottawa, Ontario
K1A 0L8
Security-Policy_Politiques-sur-la-Securite@cbsa-asfc.gc.ca

Mar 13/07

# CBSA SECURITY MANUAL – CHAPTER 27 – APPENDIX A:

## MANAGERS' GUIDE TO CONDUCTING INTERNAL INVESTIGATIONS

Internal Affairs Section
Corporate Security and Internal Affairs Division
Comptrollership Branch June 2006

---

TABLE OF CONTENTS

14. ENQUIRIES

---

## 1. FOREWORD

Canada Border Services Agency (CBSA) managers are responsible for managing CBSA programs and services in a manner consistent with public expectations regarding public funds and resources. CBSA employees must comply with the legislation and regulations administered by the CBSA, the CBSA Code of Conduct, as well as approved procedures. Management and employees have a role in the protection of public resources and funds from employee misconduct or abuse. When an incident involving an employee or allegations of misconduct are brought to management's attention, each incident must be thoroughly investigated by Internal Affairs (IA) or by local management after discussion with IA. Because incidents often affect more than one area of responsibility, a co-ordinated effort between management and IA is vital. It is in keeping with this spirit of cooperation that this guide was developed.

## 2. OBJECTIVE

This guide provides functional guidance to all levels of management with respect to the reporting of alleged or suspected employee misconduct to Internal Affairs; it also provides direction to managers on how to conduct fair and thorough internal investigations.

## 3. RESPONSIBILITIES

**Directors** are responsible for promptly reporting to the Manager, Internal Affairs, all allegations of employee misconduct or incidents without fail. Items to be reported are as specified in the **CBSA Security Manual, Security Volume, Chapter 27 -** ***Internal investigations into alleged or suspected employee misconduct or any other incident which could effect the public trust in the CBSA or its working relationship with other law enforcement partners.*** When apprised of an allegation of employee misconduct, the Director or his delegate will conduct a preliminary inquiry by gathering information to determine whether based upon the balance of probabilities the allegation is founded or not. If there is sufficient evidence to presume that the allegation is founded, the Director will report the matter to the Manager, Internal Affairs without delay. Following consultation the Manager, Internal Affairs will determine whether the matter would best be investigated locally or whether Internal Affairs will investigate the matter. In requesting an investigation, Directors must clearly state the purpose of any investigation and shall provide a written request, to IA accompanied by the report of the preliminary inquiry. When it has been agreed that local management is to conduct the investigation, Directors shall provide IA with a copy of the investigation report and of its conclusions. The fact that an investigation is being conducted by others, for example, a police force, an auditor, or Investigations Division, or that criminal or civil proceedings have been instituted in no way diminishes or negates the Director's responsibility to examine any workplace-related issue and take appropriate action.

**Managers** are required to report to their Director any allegation of employee misconduct. When a Director delegates the responsibility of a preliminary inquiry to a manager, he or she must attempt to confirm the facts pertaining to the offence, determine the potential scope of the offence, identify all parties involved, including witnesses, obtain, review, examine, and analyse related documents, and report findings to the Director. Care must be exercised to ensure that parties involved in a potential incident are not made aware that the incident is under review.

**Employees** must comply with all laws and regulations administered by the CBSA, as well as the approved rules and procedures, and abide by its Code of Conduct, thereby maintaining CBSA's integrity and that of its employees. Employees must promptly report, either orally or in writing, any allegation or suspicion of misconduct by another employee to their immediate supervisor, to one of the line supervisors, or, if the circumstances warrant it, to their Director. Furthermore, employees have an obligation to attend the interview, as well as to cooperate and assist in the conduct of an investigation into an incident or allegation of employee misconduct. This includes affording complete access to the CBSA information systems, documents, and records, to the extent that such access is legally permitted.

**Investigators** are responsible for having a clear understanding of the mandate and purpose of the investigation, obtaining all relevant preliminary information relating to the incident or allegation, identifying written sources of information and the individuals who can supplement or corroborate the available information, planning the investigation, meeting with witnesses and gathering evidence, informing the respondent that an investigation is being conducted, interviewing the respondent, and writing a clear and comprehensive report that will allow management to make an informed decision in the matter.

The **Internal Affairs Section** is responsible for providing qualified investigators to conduct investigations, advising local management on the conduct of the preliminary inquiry, and following investigations conducted by local management.

## 4. DEFINITIONS

**Complaint:** A formal allegation of employee misconduct made to or by a CBSA manager.

**Complainant:** A person making an allegation of employee misconduct.

**Fraud:** An act whereby an employee obtains a material advantage by unfair or wrongful means.

- **Incident (examples)** Allegations of misconduct made by a member of the public or by an employee against an employee;
- Alleged or suspected employee misconduct with respect to violations of criminal

laws or other laws, rules, and regulations administered by the CBSA;

- Breach of trust;
- Conflict of interest;
- Contravention of the CBSA's *Electronic Networks Policy*;
- Destruction of documents in contravention of section 67 of the *Access to Information Act*.
- Fraudulent claims regarding travel expenses, overtime and leave, including falsification of official documents, records, and medical certificates;
- Fraudulent use of the CBSA systems, such as ICES, FOSS or CPIC,
- Reduce the amount owed by a traveller, or to increase the amount of refunds or credits paid under a benefit program, to which the client is not entitled;
- Loss, theft or destruction of revenue, money, seized or abandoned goods, CBSA assets, or sensitive information;
- Participation in smuggling activities;
- Affiliation with Criminal organizations;
- Unauthorised access to and/or disclosure of confidential CBSA information.

**Investigator:** A duly appointed person who investigates allegations or incidents involving one or more employee.

**Investigation:** A systematic and thorough process involving the examination of circumstances surrounding an incident or allegation, the purpose of which is to establish and document all the relevant facts, and to analyse these in order to allow management to make an informed decision.

**Misconduct:** Any action whereby an employee wilfully contravenes an act, a regulation, a rule, a CBSA policy, an approved procedure, or the CBSA Code of Conduct Or participated in an activity which brings the CBSA into disrepute or effects the CBSA's interrelationship with other law enforcement organizations

**Preliminary inquiry:** The act of obtaining all details relating to the facts and circumstances of a reported incident, examining the documentation available in order to determine whether an allegation is substantiated, and establishing the scope of an investigation.

**Respondent:** An employee against whom an allegation of misconduct has been made.

**Witness:** An individual other than the respondent being interviewed for the purpose of obtaining information, that includes documentation, relating to a case.

**5. GENERAL**

A determination between the Manager, Internal Affairs and a Director, or a delegated manager, shall be made as to who will conduct the investigation into the incident, in light of the nature and seriousness of the incident. Incidents such as the theft of revenue, money, seized, detained, or abandoned goods, or CBSA assets or fraud, where it is suspected that an employee is responsible, are normally investigated by IA.

In agreement with the Manager, Internal Affairs, local management may conduct the investigation into employee misconduct; however, Internal Affairs will provide advice, follow the investigation, and receive a copy of the investigation report.

**6. IMPORTANCE OF ACTING PROMPTLY**

Aside from the responsibility to provide for the protection and safety of employees and to safeguard public resources, managers are also responsible for dealing effectively with allegations of employee misconduct. It is crucial that management act promptly and when informed of an incident or allegations involving an employee.

Prompt action on the part of management reduces the risk or possibility of: additional loss of public assets and/or funds; destruction of documents; and loss of confidence in accountability and the public trust. It sends a clear message to all employees that management takes allegations of misconduct involving its employees seriously; it demonstrates management's commitment to fulfilling its responsibilities and allows it to improve policies and procedures, identify training requirements, and reinforce the CBSA's commitment to making employees accountable.




---

**7. PRINCIPLES**

An investigation is a means of establishing factual and documented findings on the basis of which an informed management decision can be made. Every investigation is conducted in a rigorous and professional manner. However, the scope of investigations may vary according to the seriousness of the incident and the supporting evidence. The investigation will determine whether there is a need for policy or procedural changes, training, or disciplinary action. The investigator may contact the police if the findings reveal that the *Criminal Code of Canada* was contravened. Furthermore, delegated authority or security clearances may be suspended during an investigation, or revoked indefinitely the result of an investigation and this may negatively affect the current or future employment status of an individual within the federal government.

Investigations must be objective, thorough, and conducted by a qualified person who is aware of the rights of those involved. The events and circumstances relating to an incident, both positive and negative, must be recorded and reported accurately. Investigations are to be conducted in a timely and efficient manner. These principles are vital in order to maintain the trust of employees, their representatives, management, and the public.

## 8. TYPES OF INVESTIGATIONS

There are usually three basic types of investigations: a preliminary inquiry, an administrative investigation, and a criminal investigation, which is normally conducted by the police agency having jurisdiction.

### 8.1 Preliminary inquiry

The purpose of a preliminary inquiry is to determine whether there is sufficient evidence to support the allegations made and to make a preliminary determination of the scope of the alleged offence. In short, the preliminary inquiry involves obtaining from the individual who make the allegations as many details as possible regarding the facts and circumstances reported and to examine the documentation as thoroughly as possible. The steps in a preliminary inquiry will vary according to the type of allegation made. Steps may include such activities as reviewing an Audit Trail Search report, phone records, travel expense claims, overtime and leave forms, as well as identifying all possible parties involved and all possible witnesses. Documents must be analysed in order to make a *prima facie* determination as to whether the allegation is founded. Discretion and tact are required throughout the preliminary inquiry in order to minimise stress for those involved and for other staff. It is important that documents be safeguarded in the event that an administrative or criminal investigation is warranted.

If a preliminary inquiry supports the allegation, all attempts at gathering information should be stopped immediately, and the matter should be referred to Internal Affairs. IA will then decide, with local management, if an investigation is warranted and who should conduct it.

The decision to meet with the respondent immediately after the preliminary inquiry is matter of judgement and should be discussed with IA. In some cases, allegations are the subject of criminal investigations and any disclosure of information to the respondent could compromise this investigation as well as the administrative investigation.

### 8.2 Administrative investigation

A preliminary inquiry may determine that the allegations raised may have some basis in fact, that the misconduct is of a serious nature, that several witnesses must be interviewed, that the allegations are of a very sensitive nature or could tarnish the CBSA's credibility in the eyes of the public. In such cases, the Director may decide that an administrative investigation is warranted and will discuss the case with Internal Affairs to determine who will conduct the investigation. If the investigation concludes that there was no employee misconduct, the respondent is to be informed accordingly in a timely fashion. If an allegation of misconduct is substantiated, management is responsible for taking the appropriate

disciplinary measures.

**8.3 Criminal investigation**

In accordance with Treasury Board Policy, if the administrative investigation reveals that a CBSA employee has committed fraud, or any other offence or illegal act against the Crown, the matter must be referred to the police agency having jurisdiction that will determine whether the case warrants a criminal investigation. Criminal proceedings are the exclusive responsibility of authorised law-enforcement agencies. When a case is referred to the police, IA is responsible for monitoring the investigation and ensuring CBSA's interests are adequately protected.

If the CBSA Investigations Division conducts an investigation in respect of an employee suspected of violating the *Customs Act*, or the *Excise Tax Act*, management and IA are to be informed of the results of its investigation in order to determine whether an administrative investigation is warranted.

## 9. PRIVACY/ACCESS TO INFORMATION REQUESTS

Any Canadian citizen or permanent resident including the news media may make requests for release of information. Anyone involved in a preliminary inquiry or an investigation may obtain access to the investigation file and report under the *Access to Information Act* or the *Privacy Act*. However, requesters will only receive information to which they are entitled. Furthermore, when an administrative investigation is being conducted, only information that will not hinder the ongoing investigation will be released.

Personal information collected during an investigation may only be used for the purpose of which it is collected or for a purpose set out in the *Privacy Act*. Personal information contained in investigation files cannot, without the individual's consent, be used or disclosed except in accordance with Subsection 8 (2) of the *Privacy Act*.

The investigator must be made aware that all documentation (including tape recordings, hand-written and interview notes, documentary evidence) is subject to the *Access to Information Act* and the *Privacy Act* and that he or she is responsible for ensuring their availability should they be requested under the aforementioned legislation.




---

## 10. RETENTION OF INFORMATION

The investigator must file and retain in a secure location all files, documents, written notes, recordings, evidence, and supporting documents used during an investigation. From a legal standpoint, it is important that strict control be maintained over the storage of, and access to, this information. The items and documents gathered by the investigator to establish the facts of a case must be stored and handled in such a way as

to prevent damage and to ensure that they are properly identified and can serve to subsequently prove the chain of evidence custody as required by the legislation. The date, time, and origin must be indicated on exhibits. In most cases, exhibits serve to corroborate the testimony of witnesses. The investigator must remember that the exhibits are also subject to the *Privacy Act* or the *Access to Information Act.*

Document originals must be obtained. All copies of originals will have to be certified by the investigator. Documentation gathered for an investigation must be retained in accordance with the CBSAs Disposal and Retention Schedule. The documentation must be kept for at least five years after the case is actually closed or after the date of the last document placed on the file.

## 11. CONDUCTING AN INVESTIGATION

It is important that all activities relating to an investigation be carried out with tact and discretion. It is equally important that employees be treated with dignity and respect and be treated fairly by the investigator. Among other things, the investigator must provide the respondent with the opportunity to respond to the allegations and to defend him or herself. The following is a suggested methodology for conducting an investigation.

### 11.1 Purpose of investigation

To collect all facts and evidence relating to an allegation or an incident. It is essential that the allegations be clearly and completely stated. The purpose is not to merely *"explain away"* an incident but to supply management with the information required to determine what corrective measures, if any, are to be taken. *(Administrative or disciplinary)*

### 11.2 Planning the investigation

Based on the stated allegations, before starting interviews, the investigator must determine what must be done in order to obtain the information that will enable him or her to fully understand the circumstances and be able to report to management (*Who, What, Where, When, Why and How*). The investigator should obtain all relevant information and documentation from the resource person, usually the person who conducted the preliminary inquiry. When planning the investigation, the investigator must determine what information is missing and where it can be obtained, and identify the individuals who can supplement this information or corroborate the information available and the relevant facts. Such individuals could include supervisors who have met with the respondent to explain the directives to follow or the code of conduct by which to abide.

The investigator must define the steps to follow for the investigation, prepare the questions to be asked during interviews, estimate the time required for each interview, and carefully determine the order in which the interviews will take place. All persons who may have relevant

testimony to give must be interviewed. When it is impossible to interview someone, the investigator must note in his or her investigation report the steps taken to interview this person and the reasons why it was impossible to do so. Normally, the complainant is the first to be interviewed and the respondent is the last.

Customarily, the investigator contacts each witness the day before the interview to inform him or her of the reason for the interview, the time and place of the interview, and that her or she may be accompanied by an observer, providing the chosen observer will not be interviewed in the course of that same investigation. Witnesses should be asked to bring with them any documentary evidence they have in their possession that relates to the investigation. In exceptional circumstances individuals to be interviewed will not be contacted the day prior if to do so would negatively impact either employee safety or the investigation in question.

When planning the investigation, the investigator should therefore allow time for unforeseen delays or unplanned interviews. When such unforeseen interviews are required, it is not always possible to inform the witness one day ahead. However as much time as possible should be given in order for the witness to gather any relevant information and, if desired, obtain the services of an observer.

### 11.3 Location of interviews

The best location is the one where interruptions and distractions are fewest and the atmosphere encourages conversation. Whenever possible, a discreet office within a CBSA office should be used. Investigators must follow basic courtesies and show appropriate respect for the environment when interviewing a witness at his or her residence.

Members of the general public should not be interviewed at work when they do not find this appropriate. Such witnesses should be interviewed in a neutral location.

### 11.4 Third party presence

Any person being interviewed may, if so desired, be accompanied during the interview by a person of his/her choice as long as this person is not or will not be a witness in the investigation. Allowing the presence of an observer is a privilege and should not be considered a right. The third party present during the interview is not allowed to interfere in any way with the interview process; the third party's role is limited to that of an observer.

### 11.5 Administrative caution

At the beginning of the interview, the investigator will remind the person

to be interviewed, when the latter is not accompanied by anyone, that an observer can accompany him or her. If someone accompanies the person interviewed, the investigator will confirm that the observer is present at the request of the person to be interviewed.

All persons interviewed are to be informed:

- Of the reason for the interview;
- Of the mandate that was given to the investigator;
- That notes will be taken during the interview;
- That the person interviewed will be asked to review the investigator's notes for accuracy and, if required, corrections will be made when clarification is required;
- That the person interviewed will be asked to sign the last page and initial the others;
- That the information provided during the course of the interview may be included in the investigation report to be forwarded to the appropriate Vice President and a copy thereof to be forwarded to the Director responsible for the office where the respondent works, and may be used in a disciplinary hearing should one result;
- That the information provided during the interview will be accessible to those who are entitled to receive it under the *Access to Information Act* and the *Privacy Act* and who request it;
- That they will be asked to sign a form confirming they understand the above.

The investigator must ensure that the person being interviewed clearly understands the purpose of the meeting. The investigator will also have to answer all questions relating to the procedure to be followed.

**11.6 Confidentiality**

No assurances can be given to witnesses that their name and the information they provide will not be revealed to others, as CBSA administrative investigations are subject to the *Privacy Act*. Witnesses must be informed that investigators cannot conceal relevant information, including the sources that give credibility to the evidence gathered. Personal information learned during an investigation, which does not relate to the investigation must be discarded and never discussed with anyone during or following the investigation.

The investigator must treat all witnesses; including those he or she knows well, in a professional, impartial, and impersonal manner.

**11.7 Documenting interviews**

The questions must be open so that the person being interviewed can give his or her version of the facts. More specific questions may also be asked

in order to clarify the testimony. When the person being interviewed uses expressions such as «I believe that» or «that may be the case,» the investigator will have to clarify such statements, in order to ensure that what is being provided as fact and not impressions. The investigator should not provide his or her questions ahead of time, as they should only serve as a guide and can be changed during the interview. As needed, the investigator will have to confront the witness or the respondent with documents or other testimony previously obtained, without being threatening or intimidating. The investigator will therefore have to have the relevant documents with him or her and be ready to use them.

The investigator will take notes during the interview. It is not necessary to write down a word-for-word account, but the notes will have to accurately reflect the testimony given by those interviewed. These notes may be the only means by which the interview will be documented. Consequently, they must be dated, complete, legible, and understandable, and be placed in the investigation file.

Should the person interviewed request permission to record the interview; it is recommended that the interviewer also arrange to record the interview, while at the same time making notes of questions asked and answers provided.

The individuals interviewed will have to read the notes and attest that they constitute an accurate account of the interview. They will sign and date the document, indicating that the notes constitute a complete record of the interview. If someone refuses to sign the document, the investigator will have to sign at the end of the notes to attest that the said individual had the opportunity to review the notes and that this person was asked to sign the document but that he or she refused to comply. When requested, a copy of the signed interview notes will be forwarded to the person interviewed once the investigation is completed.

Whenever a person being interviewed provides statements pertaining to a third party, such comments will not form part of the investigation nor will they be included in the investigation report unless the third party in question has been afforded the opportunity to provide his or her response to such statements. Similarly, the report is not to reflect any comment or reference to a person or a document unless such reference is duly documented on the investigation file.

When information is obtained during a telephone conversation, the investigator must clearly note the date and time of the interview, as well as the name, title, address, and telephone number of the person interviewed. After the conversation, the investigator will read the account of the telephone conversation in order to confirm its accuracy and will

then sign the pages of notes.

**11.8 Information obtained from a third party**
When a person being interviewed provides information obtained from a third party, such information cannot be included in the report unless the investigator can identify the third party and interview the person who is the subject of the said comments.

**11.9 Refusal to cooperate**
During an investigation, should an employee refuse to be interviewed or provide the information required in the investigation, the employee in question should be informed of his or her obligation to cooperate and that a refusal could result in disciplinary action by management. The investigator shall inform the employee that the relevant CBSA manager will also be informed of the refusal to cooperate and that the refusal to cooperate will be noted in the investigation report.

During the interview, the respondent may be reluctant to discuss a situation or relate the facts thereof if he or she feels that doing so may incriminate him or her. While informing the respondent that he or she is not obliged to answer the questions, the investigator must explain that, in such cases, management will nevertheless have to render a decision without the benefit of the respondent's version.

**11.10 Report**
The investigation report is a narrative that provides those who «need to know» or who «have a right to know» with all the information required to make a final determination. The report shall be presented in a logical, clear, and concise manner that excludes personal opinions, editorial comments, and irrelevant information. However, the investigation report must include all relevant facts, including circumstantial factors that will allow management to clearly understand all aspects of the case. **The report must be presented in the following format:**

**Background:** Brief summary of the events that gave rise to the investigation.

**Example:** On (date), XX (name and title) met with XX (name, title, office)/spoke to XX (name, title, office) on the phone and alleged that (name, title, and office of respondent) had... A preliminary inquiry conducted by (name, title, office) has determined that... In light of the foregoing, the director (name and title) has asked XX (name and title) or the Internal Affairs Division to conduct an investigation.

**Purpose of the investigation:** Specify what the investigation will attempt to demonstrate.

**Example:** Ascertain the accuracy of the allegation that... or: Determine the

circumstances surrounding (description of event).

**Persons interviewed**: Alphabetical list of names (title and office, or home address for members of the public) of the persons interviewed.

**Investigation**: Testimony and evidence gathered presented in the *chronological* order in which they were obtained.

**Example**: When interviewed on (date) in the presence of (name of observer), XX (name, title, and office of the person interviewed) stated that:

- He/she saw...
- He/she observed that...
- One paragraph on each main point raised.

**Summary**: Juxtaposition of facts, testimony, and evidence, with a view to identifying flaws or weaknesses, crucial points, gaps in logic, and contradictions. All relevant information should be analysed and, as required, specific references to the documents included in the investigation file will be quoted. The ideal analysis of the facts and evidence in an investigative report should bring the reader to the same logical conclusion as that reached by the investigator.

**Observation**: (as required) Description of non-compliance with guidelines (state which ones); identification of shortcomings in procedures; the need to review, adjust, or develop a policy, directive, etc., mostly those national in scope.

**Conclusion**: Brief statement directly related to the «purpose of the investigation». It is crucial that there be a conclusion for each allegation or each incident stated in the purpose.
**Example:** Through the information obtained during the investigation, it was demonstrated that the allegation to the effect that (name, title) is believed to have (repeat allegation) was founded (or unfounded);

## 12. EXTERNAL RESOURCES

### Document Examiner

An investigator who requires the services of an expert to examine documents, samples of handwriting, etc., may refer such documents to the CBSA Laboratory.  Similarly, evidence gathered may be submitted to the RCMP's forensic laboratories or to the fingerprint lab for analysis and an opinion.

It is crucial that the investigator ensure that the expert witness is well acquainted with the relevant facts. Any opinion provided by an expert rests on facts, which the said expert presumes to be true. One should never draw any conclusions on the meaning of evidence until all the facts have been analysed. False premises can lead to flawed conclusions.

Such expert analysis and the resulting conclusions will be included in the investigation report, and the analysis portion of the investigation report will reflect the importance and relevance of the conclusion of such forensic analysis to the investigation and, if appropriate, will be cited in the conclusion.

**13. REFERENCES**

- *Access to Information Act*
- *Canadian Human Rights Act*
- *CBSA Code of Conduct*
- *Criminal Code*
- *Discipline Policy and Discipline Policy Guidelines*
- *Electronic Networks Policy Guidelines*
- *CBSA Security Manual*
- *Privacy Act*
- *Treasury Board Financial Management Manual, Chapter 4-7: Policy on losses of money and offences and other illegal acts against the Crown.*

**14. ENQUIRIES**

Should you require further information, please contact the:
Manager
Internal Affairs Section
Corporate Security and Internal Affairs Division
Canada Border Services Agency
9th floor Leima Building
410 Laurier West
Ottawa, Ontario
K1A 0L8
Telephone: (613) 948-9347
Facsimile: (613) 941-6~~0~~105




---

2014-12-12/jxs099

# Glossary of Security Terminology

## A

**Abuse** (Abus) – spoken or written words, including hardcopy or electronic messages; pictures, images or gestures that insult, disparage, revile or malign an employee.

**Abuse of authority** (Abus de pouvoir) - the act of using one's position of authority in an abusive way. This can take many forms such as taking advantage of someone or just manipulating someone with the ability to punish them if they do not comply. The act of improperly/inappropriately exercising one's power/influence over a subordinate/s through underhanded or manipulative methods.

**Access (IT)** (Accès TI) - Gaining entry to or using an electronic resource that CBSA has provided to authorize individuals. Access to such resources may be from inside or outside government premises. Access includes telework and remote access situations or where authorized individuals are using electronic resources provided by CBSA on their own time for limited personal use as defined in the policy.

**Access availability** (Disponibilité d'accès) – ensuring that legitimate users are not unduly denied access to information or resources.

**Access badge** (Insigne d'accès) - A document issued by a department/organization to show the zone or facility/complex to which the bearer has authorized access. It should not be confused with an identification card as it serves different purposes and may have a different appearance.

**Access control** (Contrôle d'accès) - access control is ensuring authorized access to assets within a facility or restricted areas by security screening employees and utilizing access control devices (i.e. keys, ID cards, access cards, security guards, etc.).

**Access control (IT)** (Contrôle d'accès TI) – provides a means of enforcing authorization policy. Access control mechanisms permit enforcement of authorization policies and determine who may access what resources and under what conditions.

**Access control methods** (Méthodes de contrôle d'accès) - the methods used to prevent unauthorized access. These methods might include person-based systems which make use of guards or receptionists, systems based on physical characteristics such as fingerprints or signatures, or systems based on access control items such as keys or proxy cards.

**Access profile** (Profil d'accès) - is the granted minimum system access privileges to an employee of the Agency to Information Technology (IT) networks/systems and information required to perform assigned work-related activities.

**Access review** (Examen de l'accès) - a user access review is a process that an organization implements to actively monitor and verify the appropriateness of an individual's access to systems and applications based on an understanding of the minimum necessary for users to perform or support business activities or functions.

**Accountability** (Responsabilisation) – the obligation to demonstrate and take responsibility for performance in the light of commitments and expected outcomes. It should be clear that accountability is not responsibility as the responsibility for work may be delegated to another individual or entity but the accountability for that work still remains with the entity making that delegation, as does the accountability for that delegation.

**Accountable COMSEC material** (Matériel COMSEC comptable) - COMSEC material that requires control and accountability within the National COMSEC Material Control System in accordance with its accounting legend code and for which transfer or disclosure could be detrimental to the national security of Canada.

**Accountable COMSEC material control agreement** (Entente de contrôle du matériel COMSEC comptable) - A binding agreement between Communications Security Establishment Canada and an entity (Government or Canadian private sector) not listed in Schedules I, I.1, II, IV and V of the Financial Administration Act that will permit the procurement, ownership, control and management of COMSEC material. It will also prescribe the conditions for the financing, resale and final disposition of the COMSEC material.

**Accreditation** (Accréditation) – the official authorisation by management for the operation of an IT system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations.

**Administrative purpose** (Fins administratives) - Is the use of personal information about an individual "in a decision making process that directly affects that individual". This includes all uses of personal information for confirming identity (i.e. authentication and verification purposes) and for determining eligibility of individuals for government programs.

**Administrative safeguard** (Mesure de protection administrative) - Refers to the enforcement of a government institution's written policies, directives, rules, procedures and processes for the protection of personal information throughout the life cycle of both the personal information and the program or activity.

**Adverse information** (Renseignement défavorable) - is information that can reasonably be cause to believe whether the individual can be relied upon not to abuse the trust that might be accorded. Is there reasonable cause to believe that the individual may steal valuables, exploit assets and information for

personal gain, fail to safeguard information and assets entrusted to him or her, or exhibit behaviour that would reflect negatively on their reliability.

**After action report** – (Compte rendu postaction) - also referred to as AAR. A document that defines the observations, strengths, weaknesses, analysis and recommendations for improvement identified during the evaluation of the exercise planning, play and support.

**After event report** (Compte rendu postévènement) - also referred to as AER. A document that provides feedback to senior officials, management, and operational staff following an event.

**After incident report** (Compte rendu postincident) - also referred to as AIR. A document that provides feedback to senior officials, management, and operational staff following an incident.

**Aggregation** (Regroupement) - the situation where a collection of assets may be categorized at a higher level of sensitivity than its component parts, due to the increased injury that could result if the aggregation is compromised; generally, aggregation applies to confidentiality, but it can also apply in certain circumstances to availability, integrity, and value.

**Alert** (Alerte) – An “instant” indication that an information system and network may be under attack, or in danger because of accident, failure or people error.

**All hazard risk assessment** (Évaluation tous risques) – a systematic approach for concurrently identifying, analyzing and estimating all natural, accidental and malicious threats and hazards.

**Alternate COMSEC custodian** (Gardien COMSEC suppléant) - The individual designated by the Departmental COMSEC Authority to assist the COMSEC Custodian and to perform the duties of the COMSEC Custodian during the temporary absence of the COMSEC Custodian.

**Alternate facility** (Installation secondaire) – a location, other than the primary facility, used to carry out business services, particularly during and/or after an emergency event. It is an alternate operating location to be used by business functions when the primary facilities are inaccessible.

**Alternate site** (Centre de repli) - an auxiliary location held in varying states of readiness and used to process data and/or deliver critical services in the event of a disruption. Note: There are four types of alternate sites: hot, warm, cold and mirror.

**Anonymous credential** (Justificatifs anonymes) - refers to a credential that, while still making an assertion about some property, status, or right of the client does not reveal the client's identity. A credential may contain identity attributes but still be treated as anonymous if the identity attributes are not recognized or used for identity validation purposes. Anonymous credentials provide clients with a means by which to prove statements about themselves and their relationships with public and private organizations anonymously.

**Anonymous internet access** (Accès à Internet anonyme) - internet access that will not identify an Agency user as an Agency user.

**Antivirus** (Antivirus) – antivirus software is specialized security software that detects known forms of malware. They are not limited to viruses, but may be ineffective against some forms such as rootkits.

**Application impact analysis** (Analyse des repercussions sur les applications) - the companion process to the Business Impact Analysis (BIA), and is the means by which IT applications, systems, and hardware can be mapped to business functions.

**Application owner** (Propriétaire de l'application) – the owner or controller of an application or group of applications who is responsible for the implementation of business rules to manage information, and for implementing and enforcing the access control policies and standards of the CBSA.

**Appropriately-screened services** (Services répondant aux normes de sécurité du personnel) - for transmittal, a messenger/courier service working under contract with the GoC where personnel are security screened, as required by the PGS, to a level commensurate with the level of information they control.

**Approved dispatch case** (Mallette à documents approuvée) - a specially designed briefcase approved by the RCMP, specifically for the transport of protected and/or classified information on commercial carriers, and designed to provide adequate resistance against surreptitious attacks in this environment.

**Approved security container** (Contenant de sécurité approuvé) - specific types of containers that have met standards established for this purpose.

**Approved software** (Logiciel approuvé) - software that has been pre-approved or certified by the CBSA/CRA/SSC for national and local systems.

**Assault** (Voie de fait) – (Verbatim from Criminal code, Section 265.1) A person commits an assault when:

a) without the consent of another person, he applies force intentionally to that other person, directly or indirectly;
b) he attempts or threatens, by an act or a gesture, to apply force to another person, if he has or causes that other person to believe upon reasonable grounds that he has, present ability to effect his purpose; or
c) while openly wearing or carrying a weapon or an imitation thereof, he accosts or impedes another person

**Asset (Biens)** – tangible or intangible things of the Government of Canada; assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.

**Asset Life Cycle** (Cycle de vie des biens) - The life of an asset is described as the point of creation, including all contracting, to the point of end of service be it by lost, stolen, encased or destroyed but not limited to those cases.

**Assurance** (Assurance) – a measure of certainty that a statement or fact is true.

**Assurance level** (Degré de certitude) - A level of confidence that may be relied on by others.

**Assurance of credential** (Assurance de justificatif d'identité) – concerns the binding of a credential to a person (without regard to their identity).

**Assurance of identity** (Assurance de l'identité) - concerns the claim that the individual is really who they say they are. Both assurances are necessary for a sound authentication solution.

**Asymmetric cryptography** (Système de chiffrement à clé publique) - a cryptographic system that relies on key pairs.

**Asymmetric cryptography** (Système de chiffrement à clé publique) - means a cryptographic system that relies on key pairs.

**ATIP** (Lois sur l'accès à l'information) – Access to Information Act gives Canadian citizens the right to access information in federal government records. The Act is closely related to security because it provides the legislative basis for the release, or exemptions from release, of government information.

**Attack** (Attaque) – any action to execute a threat.

**Attack (IT)** – (Attaque TI) - it is an attempt to exploit IT system vulnerability. Attempts to destroy, expose, alter, or disable an Information System and/or information within an information system also referred to as "Cyber Attack".

**Audit** (Physical Security) – verification that the administrative, physical, procedural and technical physical security controls have been arrived at using appropriate means and that such control meet all requirements through all phases of their life cycle or application. The standards associated with the conduct of audits are drawn from the International Association of Internal Auditors, as accepted by the Treasury Board of Canada Secretariat (TBS).

**Audit** (Program) - refers to a professional and independent appraisal function that provides objective, substantiated conclusions as to how well the organization's risk management, control and governance processes are designed and working.

**Audit log** (Journal de vérification) - is an electronic file generated by an application (word, excel, etc.), or by a computing or network device. This file contains security related information such as access history (login/logout), time and event results, and other data. Logs can contain a record of user actions and the result of those actions, providing data useful for forensic activities (e.g. multiple user authentication attempts).

**Audit trail** (Piste de vérification) - a chronological record of system activities to enable the construction and examination of the sequence of events or changes in an event (or both).

**Authentication** (Authentification) – a positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified. In simpler terms, it is the act of verifying the claimed identity of an individual, station or originator.

**Author** (Auteur) – a person who creates or collects information.

**Authorities** (Autorité) - the organization vested by the executive team with the power to develop, approve or halt the execution and work for an IT security function.

**Authoritative identity store** (Mémoire officielle des identités) - authoritative source or Identity store is the source of the data that flow down to the Identity Management System. An authoritative source or identity store is simply a directory or database that contains people's identity detail. Usually this Authoritative source contains information like employee Id, first name, last name, telephone, e-mail, department, etc.

**Authoritative source** (Source faisant autorité) - An authoritative source is one which has the ability to set down minimum requirements to which the Agency must comply.

**Authority cards** (Fiches faisant autorité) - these cards identify CBSA officers who have been granted authorities from the President for the purposes of administering (or enforcing) parts of the Customs Act and the Immigration and Refugee Protection Act (IRPA). Example: intelligence, investigations, compliance verification, hearings and inland enforcement officers.

**Authorization** (Autorisation) – the granting of the right to access an IT system by the owner or controller of an information technology system to a user, program or process.

**Authorized users** (Personnes autorisées) – includes employees of the federal government, as well as contractors and other individuals who have been authorized to access electronic networks.

**Auto-forward emails** (Réacheminement automatique de courriels) – the ability to forward or re-direct emails automatically to another email address without first opening and sending the email.

**Availability** (Disponibilité) – the condition of being accessible and usable in a timely and reliable manner to support operations, programs and services.

## B

**Background investigation** (Enquête sur les antécédents) - An inquiry into the background of an individual under consideration for employment, credit, access to sensitive assets or other reasons.

**Base building security** (Sécurité de l'immeuble de base) – security safeguards provided by the custodian department to protect a facility but not the assets contained in the building. Basic building security

provides a base or starting point for other security requirements (i.e. minimum and enhanced safeguards) to be added to protect the specific assets held by the Agency.

**Base building security attributes** (Protection de base des édifices) – security safeguards (controls) provided by the custodian department to protect a facility but not the assets contained in the building. Basic building security provides a base or starting point for other security requirements (i.e. minimum and enhanced safeguards) to be added to protect the specific assets held by the institution.

**Baseline security requirements** (Exigences de base) –mandatory provisions or measures that must be implemented and maintained in force at all times. These controls are based upon an assessment of risk and measures, promulgated under the authority of the Departmental Security Officer.

**Basic building security attributes** (Protection de base des édifices) - security safeguards provided by the custodian to protect a building but not the assets contained in the building. Basic building security attributes provide a base or starting point for other security requirements (i.e. minimum and enhanced safeguards) to be added to protect the specific assets held by the institution.

**Best practice** (Pratique exemplaire) – a method used to manage security risk that demonstrates that it both satisfies all requirements but does not in a way that is unusually or distinctly effective or efficient.

**Black key** (Clé Noire) - Encrypted key (i.e. classified keying material in encrypted format that has been encrypted with cryptography approved by Communications Security Establishment Canada).

**Bluetooth** (Bluetooth) - is a wireless short-range radio communications technology facilitating data transmission over short distances from fixed and mobile devices, creating wireless personal area networks (PANs). It most often is used to connect devices without the inconvenience of wires or wall jacks.

**Bomb threat** (Alerte à la bombe) – threat, usually verbal or written, to detonate an explosive or incendiary device to cause property damage, death, or injuries, whether or not such a device actually exists.

**Bonded carrier** (Transporteur cautionné) – a carrier who has posted security with the CBSA and who is permitted to transport, under CBSA control, between points in Canada, dutiable goods upon which duty has not yet been paid.

**Breach of information** (Infraction à la sécurité des renseignements) – an act or event that either has the potential of compromising or has breached the safeguards designed to ensure confidentiality, integrity and availability of information, systems and/or processes. A breach of information may have impacts on the privacy, businesses or on the organization.

- Privacy (Renseignements personnels) – refers to an information security incident involving personal information.
- Business (Entreprise) – refers to an information security incident involving business information.

- Organization (Organisation) – refers to an information security incident involving Agency information.

**Breach of security** (Infraction à la sécurité) - An act or omission, deliberate or accidental, that results in the actual or possible compromise of controlled goods (as defined in Part 2 of the Defence Production Act) or related technology; such breaches may include controlled goods or technology lost while being transported; controlled goods or technology left in an unsecured area where unauthorized persons have access; unauthorized disclosure by any person; theft; and loss, or exposure in circumstances that make it probable that a breach has occurred.

**Break and enter** (Introduction par effraction) – unauthorized access for criminal purposes into a facility.

**Bribery / accepting facilitation payments** (Subornation / acceptation de paiements de facilitation) - the offering, promising, giving, accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages (taxes, services, donations, etc.).

**Broadband internet access devices** (Dispositifs d'accés Internet à haut débit) – refers to devices that allow access to the internet through a greater bandwidth for faster speed.

**Business** (Entreprise) – an organization engaged in the trade of goods and/or services to consumers and is generally administered to earn profit.

**Business continuity management** (Gestion de la continuité des activités) - An integrated management process involving the development and implementation of activities that provides for the continuity and/or recovery of critical service delivery and business operations in the event of a disruption (Public Safety Canada).

**Business continuity plan** (Plan de continuité des activités) – a plan that provides the information required to minimize the impact of a service interruption and lists strategies that must be carried out to ensure an efficient and timely recovery of operations following a major disruption to business.

**Business continuity planning** (Planification de la continuité des activités) - critical services or products are those that must be delivered to ensure survival, avoid causing injury, and meet legal or other obligations of an organization. Business Continuity Planning is a proactive planning process that ensures critical services or products are delivered during a disruption.

A Business Continuity Plan (BCP) includes:

- Plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data and assets.
- Identification of necessary resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodations.

**Business continuity planning program** (Programme de planification de la continuité des activités) – is to provide for the continued availability of its critical services and assets that contribute to the health, safety, security and economic well-being of Canadians, and the effective functioning of government.

**Business impact analysis** (Analyse des répercussions sur les operations) - a business impact analysis is a tool to assess the impacts of disruptions on the department and to identify and prioritize critical services and associated assets.

## C

**Cabinet confidences** (Documents confidentiels du Cabinet) - Cabinet confidences are referenced in the Policy on the Security of Cabinet Confidences (April 2007) and include, but are not limited to draft and final versions of memoranda, discussion papers, agenda, records and draft legislation

**Canada Labour Code** (Code canadien du travail) – Part II of the Canada Labour Code on occupational health and safety provides guidance to the federal government to prevent accidents and injury. This includes measures to protect employees (e.g. prevention of violence in the workplace).

**Capability improvement process** (Processus d'amélioration de la capacité) - the whole-of-government approach to the collection and analysis of government response for exercises as well as real events and incidents.

**Categorization** (Catégorisation) - The determination of the specific type of sensitive information or sensitivity asset and the level of injury that is likely to result from the loss of confidentiality, integrity and availability of it and whether that injury would be to the national interest, an organization or an individual or any combination thereof.

**Caveat** (Mise en garde) - a marking in addition to the level of confidentiality that indicates access limits or special handling measures.

**Certification** (Certification) – a comprehensive evaluation of the technical and non-technical security features of an IT system and other related safeguards to establish the extent to which a particular design and implementation meets a specific set of security requirements, made in support of the accreditation process.

**Certification authority** (Autorité de certification) - a person or entity that issues digital signature certificates and that is listed as such on the website of the Treasury Board Secretariat.

**Chain letters** (Chaîne de lettres) - are e-mail messages with a single intent: to have you forward them to others. They falsely offer luck, money or a wish if you send them on.

**Chat rooms** (Bavardoirs) - are electronic forums where participants can have on-line discussion in real time, normally through the exchange of text messages with each other.

**Classes of personal information** (Catégories de renseignements personnels) - refers to personal information that is not used administratively or not retrievable by personal identifier—for instance, unsolicited opinions or general correspondence may be categorized under classes of personal information.

**Classified assets** (Biens classifiés) – assets whose compromise would reasonably be expected to cause injury to the national interest.

**Classified information** (Renseignements classifiés) – information related to the national interest, which concerns the defence and maintenance of the social, political and economic stability of Canada that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest if the information is compromised.

- Confidential (Confidentiel) – Injury to the national interest if compromised (information related to negotiations with provinces, strategies, tactics, political and economic report on other nations, not publicly available in Canada).
- Secret (Secret) – Serious injury to the national interest if compromised (minutes or records of Cabinet Committees, draft legislation, tactics relating to international negotiations, case files with national security implications).
- Top Secret (Très secret) – Exceptionally grave injury to the national interest if compromised (important and significant negotiations, vital law enforcement and intelligence matters, information classified by CSIS and RCMP regarding criminal or security threats.

**Client** (Client) - the intended recipient for a service output. External clients are generally individuals (Canadian citizens, permanent residents, etc.) and businesses (public and private sector organizations). Internal clients are generally public service employees and contractors.

**Client information** (Information sur la clientèle) - information, from or about clients, of any kind and any form obtained or created by or on behalf of CBSA, but excludes information that does not reveal, directly or indirectly, the identity of the client to whom it relates unless it would disclose a trade, business, industrial, commercial or professional secret or trade process.

**Communication infrastructure failure** (Défaillance de l´infrastructure de communication) – interruption of telecommunication devices, services or programs.

**Communications intelligence** (COMINT) (Renseignement sur les communications) – technical information or intelligence derived from the exploitation of communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those systems or networks by other than the intended recipient.

**Communications intelligence control** (Surveillance du renseignement sur les communications) – administration and coordination of client support services to manage and maintain compartmented Security Clearances, security and integrity of SIGINT Secure Area (SSA), and Special Intelligence Material.

**Communications intelligence control officer** (COMCO officer) –(Agent de surveillance du renseignement sur les communications) - is responsible for the management and oversight of classified and sensitive information related to National intelligence interests that has been identified and designated as Special Material. Special Material is all information and material that requires special control for restricted handling under compartmented foreign intelligence systems. Special Material includes (but is not limited to) Signals Intelligence (SIGINT).

**COMSEC Communications Security** (Sécurité des communications) – The application of cryptographic security, transmission and emission security, physical security measures, operational practices and controls to deny unauthorized access to information derived from telecommunications and that ensure the authenticity of such telecommunications.

**Compartmentalization** (Cloisonnement) – dividing a facility/floor space into smaller areas and controlling the access to each. Individuals are given access privileges only to areas to which they require access to perform their job.

**Complainant** (Plaignant) – is a person making an allegation of employee misconduct.

**Complaint** (Plainte) – means an allegation or suspicion of misconduct by an employee.

**Compliance** (Conformité) - refers to the ability to reasonably ensure conformity and adherence to organization policies, plans, procedures, laws, regulations, and contracts.

**Component** - (Composant) - constituents of a system.

**Compromise** (Compromission) – the unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information.

**Compromise of security controls** (Compromission des mesures de protection) – compromise of security measures used to protect assets, information and employees resulting in increased threats and vulnerabilities (passwords, encryption keys, locks, etc.).

**Compromise/interruption** (Compromission et interruption) – services, programs or activities that are terminated, disturbed or paused unexpectedly resulting in a loss of productivity or an interruption of service.

**Computer virus** (Virus informatique) - a computer virus is a type of malware that, when executed, replicates itself into other computer programs or data files, and performs some type of harmful activity on infected hosts.

**COMSEC account** (Compte COMSEC) - an administrative entity identified by an Electronic Key Management System Identifier (i.e. COMSEC Account number), used to maintain accountability, custody and control of COMSEC material that has been entrusted to the entity.

**COMSEC account audit** (Vérification de compte COMSEC) - independent cooperative examination of a COMSEC Account's records and activities to ensure COMSEC material produced by or entrusted to the COMSEC Account is handled and controlled in accordance with applicable directive.

**COMSEC authority (**Autorité COMSEC) – the individual is responsible for the security and accountability of COMSEC information and assets and develops Agency COMSEC policy and standards and provides advice regarding COMSEC requirements.

**COMSEC courier certificate** (Ordre de mission de messager COMSEC) - a document authorizing an individual to transport COMSEC material.

**COMSEC custodian** (Gardien COMSEC) - the individual designated by the Departmental COMSEC Authority to be responsible for the receipt, storage, access, distribution, accounting, disposal and destruction of all COMSEC material that has been charged to the departmental COMSEC Account.

**COMSEC equipment** (Équipement COMSEC) - Communications Security Establishment Canada approved cryptographic equipment and systems designed to protect classified or PROTECTED C information and data for the Government of Canada. It may also include crypto-ancillary, crypto-production and authentication equipment.

**COMSEC facility** (Installation COMSEC) – an authorized space in a building or other location that is employed for the purpose of generating, storing, repairing or using COMSEC material.

**COMSEC incident** (incident COMSEC) - tout événement qui met en péril ou pourrait mettre en péril la sécurité de renseignements classifiés et protégés du GC pendant leur stockage, leur traitement, leur transmission ou leur réception durant le processus de télécommunication.

**COMSEC material** (Matériel COMSEC) - material designed to secure or authenticate telecommunications. COMSEC material includes - but is not limited to - keys, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items performing COMSEC functions.

**COMSEC sub-account** (sous-compte COMSEC) - an administrative entity identified by an Electronic Key Management System Identifier (i.e. COMSEC Account number) established by a COMSEC Account to assist in the control of the COMSEC material entrusted to the COMSEC Account.

**Confidential** (Confidentiel) - applies to information when its compromise could reasonably be expected to cause injury to the national interest of Canada. Examples include information related to negotiations with provinces, strategies, tactics, political and economic report on other nations, not publicly available in Canada. Documents at the Confidential level are strategy papers on interest rates and inflation policy, or records of discussions of federal interdepartmental committees

**Confidentiality** (Confidentialité) - is the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the Access to Information Act and the Privacy Act (Privacy of information).

**Conflict of interest** (Conflit d'intérêt) - a situation in which an employee has private interests that could improperly influence the performance of his or her official duties and responsibilities or in which the employee uses his or her position for personal gain. A real conflict of interest exists at the present time, an apparent conflict of interest could be perceived by a reasonable observer to exist, whether or not it is the case, and a potential conflict of interest could reasonably be foreseen to exist in the future.

**Consequence scenarios** (Scénarios sur les conséquences) – scenarios designed to simulate a wide range of potential emergency effects on the organization. These scenarios are used to provide the context for all continuity management planning efforts.

**Consistent use** (Usage compatible) - Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

**Consolidated User Administration** (Administration centralisée des comptes d'utilisateurs) - consolidate user and security administration management for accessing CRA / CBSA applications.

**Constructing facilities** (Construction d'installation) – facilities built by the Crown and facilities built for the Crown by private sector landlords.

**Content administration** (Administration de contenu) - may include, but is not limited to, installing out of office messages or extracting corporate documents.

**Content monitoring** (Contrôle du contenu) - may include, but is not limited to, viewing the content and analyzing the volume of files, e-mail messages or logs to determine whether misuse has occurred.

**Continued** (Continu) – can be interrupted but must be restored within an acceptable timeframe.

**Continuity management** - (Gestion de la continuité) – a comprehensive approach to ensure the Agency's ability to achieve its core objectives in the face of adversity. This means not only reducing the impact of unexpected disruptions, but also ensuring the ability and speed of the organization to effectively recover from emergencies.

**Continuity management process** - (Processus de gestion de la continuité) – comprehensive strategic and systematic process to support the identification and analysis of business services, infrastructure and interdependencies for the development of continuity management plans.

**Continuous** (Permanent) – must have no interruption.

**Continuous monitoring** (Contrôle continu) - checking of the monitored assets by personnel in control of the assets, guards or electronic means with enough regularity to detect attempted unauthorized access.

**Control of access** (Contrôle de l'accès) – ensuring authorized access to assets within a facility or restricted areas by security screening employees, visitors and material at entry points by employees, guards or automated means and, where required, monitoring their movement within the facility or restricted access areas by escorting them.

**Controlled area** (Zone controlee) - A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

**Controlled assets** (Biens contrôlés) – Refers to assets that have been assessed as requiring specialized internal security controls that are integrated into ongoing operations throughout their life cycle from procurement and issuance, to transit, repair, maintenance, return and disposal. Examples of controlled assets include, but are not limited to, badges, identification cards, authority/designation cards, firearms/ammunition and CBSA stamps.

**Controlled cryptographic item marking** (Mention article cryptographique contrôlé) – a marking applied to COMSEC material that serves as a warning that material so marked is subject to special handling and control requirements.

**Controlled cryptographic items** (Articles crytographiques contrôlés) - are link encryption devices endorsed by the Communications Security Establishment Canada (CSEC) and used to protect the confidentiality and integrity of Protected C and classified information while transmitted over electronic means. Two compatible CCI are required to establish a secure link.

**Controllers/facilitators** (Contrôleur/animateur) - trusted agent who manage exercise conduct. They direct and monitor the pace and intensity of exercise play to ensure that exercise objectives are achieved and safety and security are maintained.

**Controlling authority** (Autorité de contrôle) - designated entity responsible for managing the operational use and control of key assigned to that cryptographic network.

**Corporate information** (Renseignement de l’organisation) - corporate information is recorded information derived from the actions, transactions, business processes, functions and activities of the CBSA.

**Creation of personal information** (Création de renseignements personnels) - refers to any personal information element or sub-element that a government institution assigns to an identifiable individual regardless of whether the information is derived from existing personal information under the control of the government institution or the institution appends new information to the individual.

**Credential** (Justificatif d’identité) - a unique physical or electronic object (or identifier) issued to, or associated with, an individual, organization or device.

**Credential assurance** (Assurance des justificatifs) - the assurance that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, modified).

**Credential assurance level** (Niveau d'assurance des justificatifs) – The level of confidence that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).

**Credential risk** (Risqué lié aux justificatifs) – The risk that an individual, organization or device has lost control over the credential that has been issued to him or her.

**Criminal association** – (Association criminelle) - association with individuals or groups who are believed or known to be connected with criminal activities. This limitation on association covers any social, sexual, financial, or business relationship with a source of information, a suspected or known criminal, or an illegal person subject to being removed from Canada.

**Criminal record name checks** (Vérification nominale du casier judiciaire) - A criminal record name check is a search that is used to determine whether an individual has a criminal conviction for which a pardon has not been granted. A criminal record check is performed against the national repository of criminal records maintained by the Royal Canadian Mounted Police (RCMP.

**Crisis** (Crise) – a period of danger for the government, resulting from a natural or man-made mishap, debacle or disaster. A crisis need not pose a serious threat to human life, but it must somehow challenge the public's sense of appropriateness, tradition, values, safety, security or the integrity of the government.

**Critical asset** (Bien essentiel) – an asset, supporting a critical service, whose compromise would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the GoC.

**Critical business function** (Fonction opérationnelle essentielle) is a specific function or on business process that, if interrupted, has a major impact on staff and operations and adversely affects the mandate and business lines of the Agency.

**Critical infrastructure** (Infrastructure critique) - The processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and to the effective functioning of government. Critical infrastructures are vital to the Agency to the extent that the incapacity or destruction of such systems and networks would have a major impact for the continuous delivery of services.

**Critical service** (Service essentiel) - a service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada (GC).

**Critical service disruption** (Interruption d'un service indispensable) – when a critical service is interrupted/compromised in terms of availability or integrity and as a result could affect the Agency's ability to achieve its core mandate. Refer to critical service.

**Critical support service** (Service de soutien essentiel) - is an interdepartmental or intradepartmental policy or service that supports a critical service

**Critical systems** (Systèmes essentiels) - System whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the efficient functioning of the Government of Canada.

**Crypto** (Crypto) - a marking which is applied to key material indicating that items so marked are subject to specific controls governing access, distribution, storage, accounting, disposal and destruction.

**Cryptographic** (Cryptographie) – cryptography is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge – the art of encryption.

**Cryptographic logic** (Logique cryptographique) - the embodiment of one (or more) crypto-algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process(es).

**Cryptographic material** (Matériel cryptographique) - all material, including documents, devices and equipment, which contain crypto-information and is essential to the encryption, decryption or authentication of communications.

**Cryptographic network** (Réseau cryptographique) - a telecommunications network (regardless of size or number of users) in which information is protected by the use of compatible cryptographic equipment using the same cryptographic key.

**Cryptography** (Cryptographie) - the discipline that treats the principles, means and methods for making plain information unintelligible and reconverting the unintelligible information back into plain information.

Type 1 Cryptography used for encrypting "Classified" information in the National interest.

Type 2 Cryptography used for encrypting "Protected" information or sensitive information not in the "National" interest.

**Crypto-ignition key** (Clé de contact cryptographique) - a device or electronic key that can be used to unlock the secure mode of cryptographic equipment.

**Cryptoperiod** (Cryptopériode) - a specific period of time during which a cryptographic key is in effect.

**Custodian department** (Ministère gardien) – is the “department having administration of federal real property.” In the case of the Agency, this may be the Agency itself (in terms of owned property), Public Works and Government Services Canada, or a private entity. In the context of facility security, the specific relationship between these two entities is defined through the Occupancy Instrument.

**Cyber attack** (Cyberattaque) - the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information that undermines the confidentiality, integrity, or availability of a computer or of the networks and information accessible throughout it.

**Cyber event** – (Cyberévénement) - indicates the security of an information system, service, or network may have been breached or compromised, an information security policy may have been violated, or a safeguard may have failed.

**Cyber incident** (Cyberincident) - any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete or render unavailable any computer network or system resource (computer attacks, compromises and virus infections.

## D

**Damage and destruction** (Dommage et destruction) – harm or injury to property or a person, resulting in loss of value or the impairment of usefulness.

**Data corruption** (Corruption de données) – compromise of data integrity.

**Data files/equipment containing information** (Fichiers de données et matériel contenant des renseignements) – any equipment (electronic or paper) used to store or access information. (i.e. USB keys, laptops, CD, etc.)

**Data infrastructure failure** (Défaillance de l'infrastructure de données) – failure of CBSA data system

**Data matching** (Couplage des données) - Is an activity involving the comparison of personal information from different sources, including sources within the same government institution, for administrative or non-administrative purposes. The data-matching activity that is established can be systematic or

recurring. The data-matching activity can also be conducted on a periodic basis when deemed necessary. Under this policy, data matching includes the disclosure or sharing of personal information with another organization for data-matching purposes.

**Declassification** (Déclassification) – removal of the sensitivity rating (classification level) of the information or asset.

**Defalcation** (Abus de confiance) - is a misappropriation of public funds, trust funds or money held in a fiduciary capacity.

**Deficiency** (Défaillance) – a failure to meet the requirements associated with a security control that results in the personnel, assets, or operations being directly exposed to the potential of compromise.

**Delegate** (Délégué) - Is an officer or employee of a government institution who has been delegated to exercise or perform the powers, duties and functions of the head of the institution under the Act.

**Demarcation** (Délimitation) – identified physical barriers around each separate area to which access is controlled.

**Demonstration** (Manifestation) – when a group or individuals stage a demonstration outside CBSA facility as a means of expressing views and exercising political pressure.

**Denial of service** (Déni de service) - an attack that could prevent the usage of networks, systems, or applications

**Department** (Ministère) - All departments named in Schedule I, divisions or branches of the federal public administration set out in column I of Schedule I.1, corporations named in Schedule II, and portions of the federal public administration named in schedules IV and V of the Financial Administration Act (FAA), unless excluded by specific acts, regulations or Orders in Council.

**Departmental COMSEC authority** (Autorité COMSEC du ministère) - the individual designated by, and responsible to, the Departmental Security Officer for developing, implementing, maintaining, coordinating and monitoring a departmental COMSEC program which is consistent with the Policy on Government Security and its standards.

**Departmental security guidelines** (Lignes directrices minitérielles sur la sécurité) – suggested methods to implement departmental security policies, standards and procedures.

**Departmental security officer** (Agent de sécurité du ministère) – responsible for establishing and directing the Agency's Security Program.

**Departmental security plan** (Plan de sécurité du ministère) - details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving Agency security, while supporting its implementation.

**Departmental security policy** (Politique de sécurité du ministère) – generic mandatory security requirements developed and promulgated by the Security and Professional Standards Directorate.

**Dependency** (Dépendance) – the reliance of a service on internal/external services, assets and resources (including individuals).

**Deputy Head** (Administrateur général) (administrateur général) - Deputy Head as defined in section 11 of the Financial Administrtion Act, and in the case of the Canadian Forces the Chief of the Defence Staff.

**Designated information and assets** (Renseignements et biens désignés) – information and assets, the compromise of which could reasonably be expected to be injurious to the interests other than the national interest or when their confidentiality, integrity, availability or value warrant safeguarding. Designated assets could include, among others, computers, printers, fax machines, cash and negotiables, etc.

**Designated officer** (Agent désigné) - an officer who is designated by the President pursuant to subsection 163.4 of the Customs Act. Subsection 163.5 provides a designated officer with the powers and obligations afforded to peace officers for the purposes of enforcing sections 253, 254, and 495 to 497 of the Criminal Code.

**Designation card** (Carte de designation) - the President may designate any officer for the purposes of administering Part VI.1 of the Customs Act (Enforcement of Criminal Offences other than Offences under this Act), and provide the officer with a certificate of designation.

**Destruction** (Destruction) – the obliteration of information or assets. Accidental destruction of assets can occur as a result of fire, flood, earthquake or similar calamity, but may also be caused by negligence or deliberate action such as vandalism, riot, sabotage or acts of war.

**Destruction equipment** (Équipement de destruction) – any device or process used to change the medium which contains classified or protected information in such a way that the classified or protected information can no longer be read or deciphered.

**Detection** (Détection) – the use of appropriate devices, systems and procedures to signal that an attempted or actual unauthorized access has occurred.

**Detrimental effect** (Effet adverse) – loss or damage done to, or sustained by, any person or thing.

**Devices** (Dispositifs) – tools used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy information electronically.

**Digital signature** (Signature numérique) – digital signature (or public key digital signature) is a type of method for authenticating digital information analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public key cryptography.

**Digital signature certificate** (Certificat de signature numérique) - In respect of a person, means an electronic document that (a) identifies the certification authority that issued it and is digitally signed by that certification authority; (b) identifies, or can be used to identify, the person; and (c) contains the person's public key.

**Diplomatic mail service** (Service de courrier diplomatique) - a mailing service provided by the Department Foreign Affairs, Trade and Development Canada (DFATD) to provide safe and secure delivery of unclassified, protected and classified information under its control to and from missions outside Canada via diplomatic bag.

**Disability to contract** (Incapacité contractuelle) - no person who is convicted of:

a) an offence under section 121, 124 or 418, (of the Criminal Code of Canada)

b) an offence under section 380 (of the Criminal Code of Canada) committed against Her Majesty,

c) an offence under paragraph 80(1)(d), subsection 80(2) or section 154.01 of the Financial Administration Act, has, after that conviction, capacity to contract with Her Majesty or to receive any benefit under a contract between Her Majesty and any other person or to hold office under Her Majesty.

**Disaster** (Catastrophe) - a sudden, unplanned, catastrophic event that causes unacceptable damage or loss; compromises an organization's ability to provide critical functions, processes, or services for an unacceptable period of time, or compels management to divert from normal production responses and exercises its business continuity or disaster recovery plan.

**Disaster recovery plan** (Plan de reprise après catastrophe) - approved arrangements, processes, procedures, and activities to ensure that IT application systems, data and infrastructure are recovered after a disaster to operational levels acceptable to an organisation.

**Disclosure** (Divulgation) - the release of information, by any method, to any person inside or outside the department that controls the information, who is not authorized to obtain access to the information.

**Discreditable conduct** (Conduite déshonorante) - conduct on- and -off duty, which is likely to bring sufficient discredit or harm to the reputation of the employee or/and that of the Agency.

**Disruption** (Interruption) – any interruption that compromises in the availability of continued delivery, and/or integrity of the Agency's essential services.

**Diversion theft** (Vol de détournement) - Diversion theft is a "con" exercised by professional thieves, normally against a transport or courier company. The objective is to persuade the persons responsible for the legitimate delivery of goods that the goods are requested elsewhere.

**Double sealed envelope** (Sous double pli cachet) – a sealed envelope (inner envelope) appropriately addressed, security markings and includes transmittal note receipt which is placed in inner envelope, enclosed within another sealed envelope (outer envelope). Outer envelope has address only, no security markings. Inner envelope is also sealed with security tape.

**Downgrading** (Déclassement) – reducing the level of sensitivity rating (i.e. from Secret to Confidential) of the information or asset. The decision, recorded in writing, of the originator of classified information or another officer authorized by the deputy head to lower the classification level of information.

**Drills** (Exercice) - an operations-based exercise to provided training on new equipment, to develop or test new policies or procedures, and to practice and maintain current skills.

**Drug / intoxicant usage** (Usage de drogue/substance intoxicante) - this definition speaks to the fact that it is prohibited but does not necessarily "define" drug/intoxicant usage. Suggestion: the consumption of any substance deemed to be illegal and/or in contravention of the CBSA code of conduct while on- duty, in uniform (on or off-duty), operating an official vehicle, or on any premises where the CBSA conducts its business.

**Due diligence** (Diligence raisonnable) (related to audit trail records) - is a reasonable review of the audit trail records that is sufficient to assure oneself that these are in accordance with the employee's workload and duties.

**Dumpster diving** (Fouille de poubelles) – searching for invoices or other documents containing sensitive information in the trash. The searching of Agency refuse/waste by unscrupulous individuals with the intent of finding information or assets for illegal purposes.

# E

**Eavesdropping** (Interception illicite) – intentional listening to a private conversation, which may reveal information that could compromise the Agency's information and assets.

**Electronic intelligence** (Renseignement électronique) – technical information or intelligence derived from the collection, processing and analysis of electromagnetic non-communications emissions.

**Electronic key** (Clé électronique) - key that is stored on magnetic media, optical media, or in electronic memory, transferred by electronic circuitry, or loaded into COMSEC equipment.

**Electronic media** (Support électronique) - any media that use electronics or electromechanical energy for the end-user to access the content.

**Electronic networks** (Réseau électronique) – groups of computers and computer systems that can communicate with each other. Without restricting the generality of the foregoing, these networks include the Internet, networks internal to a department, and public and private networks external to a department.

**Electronic resources** (Ressources électroniques) - groups of computers, computer networks and systems, functions, or devices allocated to users or programs. These resources include the Internet, functions, software or devices internal to CBSA, and public and private functions or devices external to the Agency. Also included are any hardware such as standalone computers, laptops, peripherals, memory devices, wireless devices, and any other media used to obtain, store, disseminate information, etc. Many non-computing devices, such as digital cameras and cellular phones, are considered as electronic resources because of their capability for storing and disseminating information.

**Emergency** (Urgence) - In the context of government operations, an emergency is an event, internal or external to an organization, real or imminent in nature, which, because of its detrimental effects, and its unforeseen nature as well as the need for immediate action, could call upon an organization's ability to partially or totally modify the fashion in which it carries out its other mandated responsibilities. An emergency will usually be an abnormal situation which, to limit damage to persons, property or the environment, requires prompt action beyond what may be considered normal procedures.

**Emergency management** (Gestion des urgences) – The management of emergencies concerning all hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery.

**Emergency Management Act** (Loi sur la gestion des urgences) – sets out how to prepare, prevent, mitigate and recover when faced with national emergency situations and disruption of critical services that impact the health, safety, security and economic well-being of Canadians, Security plays an essential role in the estabishment of business continuity plans.

**Emergency management planning** - (Planification de la gestion des urgences) – a process through which emergency management plans; policies and procedures are developed, validated and maintained.

**Emergency management plans** (Plans de gestion des urgences) – are developed to ensure the safety and welfare of employees in the event of an emergency. These plans also provide procedures to effectively recover critical services after an emergency. They include: Continuity Management Plan (CMP), Emergency Response Plan (ERP) and Fire Safety Plan (FSP).

**Emergency Operation Centre** (Centre des operations d'urgence) – A designated facility established by an agency or jurisdiction to coordinate the overall agency or jurisdictional response and support to an emergency response.

**Emergency Response** (Réponse en cas d'urgence) - deals with the immediate response to the effects of any emergency; evacuating a damaged building, putting out the fire or stopping the leak.

**Employee** (Employé) - means any person working for the CBSA, including management, employees on leave without pay, trainees, recruits and students, whether indeterminate, term, casual, part-time or seconded or assigned to the CBSA.

**Employee electronic access file** (Dossier d'accès électronique de l'employé) - a file generated for purpose of monitoring employee electronic access to customs information for a specific period of time.

**Employee Notice Line** (Ligne d'information pour les employés) - the CBSA Employee Notice Line 1-866-668-4234 is to be used for getting up-to-date information about the workplace in the event of a building closure. Examples of emergency or disruption to regular operations are inclement weather, environmental disasters, local or national emergencies, demonstrations and building occupations.

**Encryption** (Chiffrement) – the transformation of clear voice or data to an unintelligible form through the use of a reversible cryptographic process accomplished either by hardware of software. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. There are two main types of encryption; asymmetric encryption (also called public-key encryption) and symmetric encryption.

**Encryption key** (Clé de chiffrement) – a passphrase or algorithm needed to encode text into cipher text.

**Enhanced safeguard** (Mesure de protection accrue) – a level of security over and above the basic accepted standard (see also Enhanced Security).

**Enhanced security** (Sécurité accrue) – a level of security over and above the basic accepted standard (see also Enhanced Safeguard).

**Entity** (Entité) – a clearly and uniquely identifiable individual, group, or organization. An entity may be an individual or may be a federal department, depending on the scope of requirements.

**Entrust** (Entrust) – an international company that provides public key infrastructure (PKI) encryption software called Entrust technologies. Entrust provides digital certificates, PKI security, and encryption software (identity management security software) for enterprises and governments.

**Essential employee** (Employé essentiel) – employee who delivers essential services.

**Essential service** (Service essential) - a service, facility or activity of the Government of Canada that is or will be, at any time, necessary for the safety or security of the public or a segment of the public.

**Evacuation** (Évacuation) – is the immediate and rapid movement of people away from the threat or actual occurrence of a hazard. Depending on the emergency, evacuations can be completed as a partial evacuation (only certain floors) or on a full scale (entire building).

**Evaluators** (Évaluateurs) - are assigned to one or more locations (if applicable) to document and evaluate individual, team, and organizational performance based on the exercise objectives and performance criteria.

**Event** (Événement) - an occurrence that takes place at a planned location and date/time (i.e. G8/G20 Summits, Olympics).

**Evidence of identity** (Preuve de l'identité) – A record from an authoritative source indicating an individual's identity.

**Excessive use of force** (Usage de force excessive) - use of force that is over and above a level then what would be appropriate under the circumstances. Authorized employees are required to limit the use of force to a level that is appropriate under the circumstances. Anything above is considered excessive use of force.

**Executive** (Cadre supérieure) - An employee appointed to the executive group (EX 01 to EX 05 levels), i.e., director, director general, assistant deputy minister or equivalent.

**Executive summary** (Sommaire) - a condensed version of the After Action Report/After Event Report/After Incident Report, designed to provide a quick overview of the report (i.e. key observations and recommendations) in no more than two pages. It is intended to provide a snapshot of the exercise/event/incident to an audience that may not have time to read the whole report.

**Exercise** (Exercice) - an opportunity to train and practice roles and responsibilities during a major event or incident in a realistic but risk-free environment. There are several types of exercises that can be conducted: orientation seminar, workshop, table top, drill, functional, and full-scale.

**Exercise aim** (But de l'exercice) - outlines the purpose of the exercise (i.e. examine CBSA's preparedness to effectively deal with the arrival of a migrant vessel).

**Exercise goal/objective** (Objectif de l'exercice) - exercise aims to achieve (i.e. identify gaps in planning, discuss reporting requirements, improve awareness of interdepartmental roles).

**Exercise purpose** (Raison d'être de l'exercice) - the reason why an exercise was conducted.

**External access network** (Réseau d'accès externe)– an internetwork that provides the network services to connect a Public Zone

# F

**Facilit**y (Installation) – a physical setting used to serve a specific purpose. A facility may be part of a building, a whole building or a building plus its site; or it may be a construction that is not a building. The term encompasses both the physical object and its use (for example, weapons ranges, agricultural fields).

**Facility security clearance (**Attestation de sécurité d'installation) – An administrtative determination that an organization is eligible, from a security viewpoint to access Classified information and assets.

**Facility Threat and Risk Assessment** (Évaluation de la menace et des risques) – installation. In relation to the building project delivery, a threat and risk assessment process evaluating the assets within a facility, the threats against them and the performance of safeguards against these threats in order to define the optimal safeguarding strategy under the circumstances. The defined strategy is used to specify the actual safeguards as the building project delivery progresses.

**Fact-finding** (Recherché des faits) - means gathering all information relevant to a complaint usually by local management in accordance with these Guidelines.

**Falsification of documents** (Falsification de documents) - the willful and fraudulent alteration, destruction or mutilation of a document to provide an opportunity to further an employee' private interests or the private interests of others.

**Family** (Famille) – spouse or common-law spouse, dependent children (including children of legal or common-law spouse), or any person permanently residing in the employee's household or with whom the employee permanently resides; for purposes of this policy, in some circumstances, it may be necessary to include family members not residing with the employee, in this definition.

**Federated identity management** (Gestion fédérée de l'identité) - the sharing of assurances of identity with trusted partners (members) of the federation.

**Federating credentials** (Fédération des justificatifs) – is the process of establishing a federation in which members share assurances of credentials with trusted members of the federation.

**Federation** (Fédération) - A cooperative agreement between autonomous entities that have agreed to work together. The federation is supported by trust relationships and standards to support interoperability.

**Findings** (Constatations) – the factual observations of a competent person with respect to the conditions found and supportable through observation, documentation or corroboration.

**Fire safety plan** (Plan de sécurité en cas d'incendie) – is a component of the Emergency Response Plan (ERP) which provides emergency response information and procedures directly related to fire.

**Firewall** (Pare-feu) – a hardware or software device that controls access in and out of a subnet. Using a set of rules, a firewall examines (filters) every packet attempting to enter or leave a network and decides if the packet can continue or not. Firewall is specialized security software that blocks or restricts access to a computer or network.

**First responder** (Premier répondant) – a person, such as a police officer, firefighter, or emergency medical technician (EMT), trained in urgent medical care and other emergency procedures and prepared to move quickly to the scene of an accident or disaster.

**For Cause** (Pour cause) – a determination that there is sufficient reason to review, revoke, suspend or downgrade a reliability status or a security clearance or site access. In the context of a security assessment, a determination whether more in-depth verifications are required.

**Foreign instrumentation signals intelligence** (Renseignement tire de signaux d'instrumentation étrangers) - technical information or intelligence derived from the collection, processing and analysis of foreign instrumentation signals by other than the intended recipient.

**Foreign national** (Étranger) - a person who is not a Canadian citizen or a permanent resident.

**Foreign State** (État étranger) – means any state other than Canada.

**Fraud** (Fraude) - Is a criminal deception involving the use of false representation with the specific intent of gaining an unfair or dishonest advantage. Fraud ordinarily involves either willful misrepresentation or deliberate concealment of material facts for the purpose of inducing another person to either part with cash or something else of value or to surrender a legal right.

**Fraud Internal** (Fraude interne) – any intentional act or intentional omission by an employee for personal enrichment, or for the enrichment of a third party, through the deliberate misuse or misapplication of the Canada Border Services Agency's resources, revenues, information, assets, or authority.

**Fraud against government** (Fraude contre le gouvernement) - intentionally deceiving the Agency in order to gain an unfair or illegal advantage (financial, political or otherwise).

**Fraud detection** (Détection de la fraude) – activities and techniques that recognize whether fraud has occurred or is occurring.

**Full-scale exercise** (Exercice complet) - an operations-based exercise that involves all emergency response functions and requires full deployment of personnel and equipment. It is a simulated emergency event, as close to reality as possible.

**Functional authority and direction** (Autorité et orientation fonctionnelles) - is the direction and performance of a particular program (i.e. designing, implementing and maintaining a program, policies and resource allocations, providing advice and guidance on the program, monitoring and reporting on program performance, etc.)

**Functional exercise** (Exercice fonctionnel) - an operations-based exercise that happens in real time with a scenario being simulated short of deploying personnel and equipment. Focuses on communication and coordination during an event or emergency.

## G

**Gambling** (Jeu) - is to bet, wager or risk money or something of value on a game of chance or mixed skill and chance. It may take many forms and includes sports pools and other types of pools.

**Government information** (Information gouvernementale) – information created, received, used, and maintained regardless of physical form, and information prepared for or produced by the Government of Canada and deemed to be under its control in the conduct of government activities or in pursuance of legal obligations.

**Graduated safeguards** (Mesures de protection progressives) – a set increasingly secure safeguards that respectively reduce risk.

## H

**Hacker** (Pirate informatique) – person who uses programming competence and knowledge of systems to gain unauthorized access to a computer or a network.

**Hacking** (Piratage) – is a term used to describe actions taken by someone to gain unauthorized access to a computer. The availability of information line on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities.

**Hand Receipt** (Accusé de réception) - an accounting record that documents the issue of and acceptance of responsibility for COMSEC material.

**Harassment** (Harcèlement) – any behaviour that demeans, embarrasses, humiliates, annoys, alarms or verbally abuses a person and that is known or would be expected to be unwelcome. This includes words, gestures, intimidation, bullying, or other inappropriate activities.

**Health and safety** (Santé et sécurité) - involves putting in place a program to ensure that employees are provided with a safe and healthful working environment. Mandated under Section 11 of the Canada Labour Code.

**Hierarchy of zones** (Hiérarchie des zones) - process by which Government of Canada departments must ensure that access to, and safeguards for, protected and classified COMSEC material are based on a clearly discernable hierarchy of zones. There are five zones: Public Zone; Reception Zone; Operations Zone; Security Zone and High Security Zone.

**High degree of injury** (Préjudice élevé) - will generally result in such things as loss of life, the breakdown of civil order (i.e. violent demonstrations), loss of territorial sovereignty, irreparable loss of public confidence, extremely large financial losses or severe disruption to the economy, disclosure of intelligence sources or methods of gathering intelligence, serious long-term damage to the conduct of international relations, and unavailability of a critical service.

**High Priority Incidents** (Incidents hautement prioritaires) – these are defined as those incidents that have impacted VERY HIGH or HIGH value assets (as described in the Harmonized Threat and Risk Assessment methodology put forward by the RCMP and CSEC in Tables B-2 and B-3 (pages B-7 and B-8 of the standard which can be found at http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf

**Hot wash** (Séance de rétroaction immédiate) - a post-exercise/event/incident debriefing session that provides involved/affected individuals the opportunity to discuss the exercise/event/incident and identify positive and negative aspects of exercise management and play, event management and/or incident response.

## I

**Identification (**Identification) – the process that enables recognition of an entity or user described to an automated data processing system. This is generally by the use of unique machine-readable names.

**Identification card** (Carte d'identité) - a document issued by the department/organization to identify the bearer. It should not be confused with an access badge as it serves different purposes and may have a different appearance.

**Identity** (Identité) – a reference or designation used to distinguish a unique and particular individual, organization or device.

**Identity and access management** (Gestion de l'identité et de l'accès) - the common term to describe the process for managing access to enterprise resources. In its basic form, IAM can be defined as a group of processes that manage "who has access to what". The processes are used to initiate, record, and manage user identities and related access permissions to CBSA information to ensure that appropriate access is provided only to those employees who require it, while limiting the access of employees who have no need for a particular information resource.

**Identity assurance** (Assurance de l'identité) – a measure of certainty that an individual, organization or device is who or what it claims to be.

**Identity assurance level** (Niveau d'assurance de l'identité) – the level of confidence that an individual, organization or device is who or what it claims to be.

**Identity claim** (Déclaration ou affirmation d'identité) – an assertion of the truth of something that pertains to a client's identity.

**Identity federation** (Fédération d'identité) - is a group of autonomous entities that have established a community to manage their clients' identity that is based on trust.

**Identity fraud** (Fraude d'identité) - is the actual deceptive use of the identity information of another person (living or dead) in connection with various frauds (including for example personating another person and the misuse of debit card or credit card data).

**Identity management** (Gestion de l'identité) – the set of principles, practices, processes and procedures used to realize an organization's mandate and its objectives related to identity.

**Identity risk** (Risqué lié à l'identité) – the risk that an individual, organization or device is not who or what it claims to be.

**Identity theft** (Vol d'identité) - is the deliberate impersonation of another person's identity. It occurs when somebody steals your name and other personal information without your knowledge. It is usually used for fraudulent purposes such as gaining access to someone's finances or committing a crime.

**Important records** (Documents importants) - Records which can only be replaced or reproduced at considerable inconvenience or expense to operations.

**Improvement action plan** (Plan d'action pour l'amélioration) - A document in table format, that identifies the observations and recommendations stemming from the After Action Report/After Event Report/After Incident Report in order to facilitate the tracking of implemented recommendations.

**Incident Action Plan** (Plan d'action en cas d'incident) - Contains objectives reflecting the overall incident strategy and specific tactical actions and supporting information for the next operational period.

**Incident Command System** (Système de commandement en cas d'incident) – A standardized on-scene emergency management concept specifically designed to allow its users to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries.

**Incident Commander** (Commandant du lieu de l'incident) – The individual responsible for the management of all incident operations at the incident site.

**Incident Management** (Gestion des incidents) - The process by which an organization responds to and controls an incident using established response procedures or plans.

**Indictable offence** (Infraction punissable par mise en accusation) – an offence described in a federal statute, which is triabal by way of indictmenent only. Indictable offences are generally considered to be the most serious criminial offences and prosecution by indictment is a lengthier and more complex court process involving preliminary hearings and trials before a judge or a judge and jury.

**Indirect collection** (Collecte indirecte) is a collection of personal information from a source other than the individual.

**Individuals** (Individus) – casuals, indeterminate employees, students and contract workers.

**Information** - (Renseignement) - is a corporate asset or resource, which is defined as data, facts or knowledge that is recorded, regardless of form, recording media or technology used.

**Information management** (Gestion de l'information) - a discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal or long-term preservation.

**Information Management (IM) Continuity Planning** (Planification de la continuité de la gestion de l'information (GI)) - As an element of the Business Continuity Planning Program, and in accordance with the Management of Government Information Policy, is the development of plans, measures, procedures and arrangements (using BCP methodology) to ensure minimal or no interruption in the availability of information assets.

**Information owner** (Propriétaire de l'information) – the owner or controller of information who is responsible for identifying the classification of their data and for implementing and enforcing the access control policies and standards of the CBSA.

**Information security** (Sécurité de l'information) - assures that the appropriate physical, technical, procedural, and psychological safeguards are afforded to information (in all its forms) beginning from the conceptualization of sensitive information through to its final and irrevocable destruction thus protecting information assets to ensure confidentiality, integrity, availability, authorization and authentication measures work effectively and consistently.

**Information security incident** (Incident de sécurité de l'information) – any unexpected or unwanted event that may cause a compromise of business activities or information security. This includes breaks in policy, failure of controls, or other previously unknown situations.

**Information Technology** (Technologies de l'information) - includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation and implementation of information systems and applications to meet business requirements.

**Information technology (IT) continuity planning** (Planification de la continuité de la technologie de l'information (TI)) – IT continuity planning identifies missions critical IT services, data, networks, systems and assets necessary to critical services and includes the development of plans, measures, procedures and arrangements (using the BCP methodology) to ensure minimal or no interruption to the availability of critical IT services and assets.

**Information technology (IT) security** (Sécurité des technologies de l'information (TI)) – the program of collective measures based on approved policies and procedures, that protect the underlying technology platforms, services, networks and applications that collect, process, store or communicate information assets.

**Information technology (IT) systems** (Systèmes de technologie de l'information) – fields of electronic data processing, telecommunications, electronic networks, and their convergence in systems; applications and associated software and equipment together with their interaction with people and machines.

**Information technology security incident** (Incident de sécurité des technologies de l'information) – any unexpected or unwanted event that might cause a compromise of business activities or information security.

**Information technology security zone** (Zone de sécurité des technologies de l'information) – a networking environment with a well-defined boundary, a security authority and a standard level of susceptibility to network threats. Types of IT Security Zone are distinguished by security requirements for interfaces, traffic control, data protection, host (device) configuration control and network configuration control.

**Infrared** (Infrarouge) – infrared (IR) radiation is electromagnetic radiation whose wavelength is longer than that of visible light, but shorter than that of terahertz radiation and microwaves.

**Injury** (Préjudice) - Injury is a detrimental effect. For protection above the normal base level to be considered, compromise of information (its unauthorized disclosure, destruction, removal, modification or interruption), must reasonably be expected to prove harmful or damaging to the specific public or private interest covered by an exemption in either the Access to Information Act or the Privacy Act. By way of guidance, classification or protection is most accurate and effective where an institution can specifically connect types of information with an identified detrimental effect on the actual parties who will suffer injury or whose interests will be damaged. This is clearly preferable to identifying some vague general harm. Another important factor is the chance or probability that an injury will occur. Basically, to determine injury, one must judge first, that a specific detrimental effect exists, and then that it is reasonably likely to follow if the information is compromised. Most exemptions under both Acts are based on a specific injury test.

**Injury as it relates to access to personal information** (Préjudice) - related to the Access to Information Act. Exemption that identifies the specific public or private interests which must be protected from injury resulting from the disclosure of information.

**Injury as it relates to assets** (Prejudice en ce qui concerne les biens) - the damage that results from the compromise of assets.

**Insider Threat** (Menace de l'intérieur) - Any person with authorized access who causes harm, intentionally or otherwise, to the assets of an organization (employee, contractor, etc.).

**Inspection** (Inspection) – a verification that all security controls are in place as required and that all statements made regarding those controls are supportable.

**Insubordination** (Insubordination) – failure or refusal to recognize or submit to the authority of a superior.

**Integrated Risk Management** (Gestion intégrée des risques) - a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective to support strategic decision making that contributes to the achievement of an organization's overall corporate objectives.

**Integrity** (Intégrité) - the state of being accurate, complete, authentic and intact.

**Internal support services** (Services de soutien internes) — Administrative services that support a department or agency, or a program; they do not include services delivered to the public or other direct program delivery services.

**Interoperability** (Interopérabilité) – the ability of federal government departments and agencies to operate synergistically through consistent security and identity management practices.

**Interruption** (Interruption) - The non-availability of service. How critical the service is to operations dictates the importance of this factor in injury and threat.

**Intervention** (Intervention) - response is the implementation of measures to ensure that security incidents are reported to appropriate security officials and immediate and long-term corrective action taken.

**Intranet** (Intranet) – a computer network, especially one based on internet technology, which an organization uses for its own internal, and usually private, purposes and that is closed to outsiders. Atlas is the home page of the Canada Border Services Agency intranet site.

**Intrusion** (Intrusion) – a type of IT security incident involving unauthorized access to, or activity on, a system or network.

**Intrusion defence system** (Système de défense contre les intrusions) – Technology that detects, alerts and where possible prevents malicious or abnormal IT behaviour from occurring.

**Inventory verification** (Vérification de l'inventaire) – a check to determine that all items are present and accounted for as represented across the various accounting systems within an organization.

**Investigation** (Enquête) – a formal, objective, systematic and thorough process involving the examination of circumstances surrounding an incident or allegation, the purpose of which is to establish, document and analyze all relevant facts in order to allow management to make an informed decision.

**Investigator** (Enquêteur) – means the person authorized by the Professional Standards Investigations Section of the Personnel Security and Professional Standards Division to investigate a complaint in accordance with these Guidelines.

**Infrared Data Association** (Association de données à l'infrarouge) - a standard for communication between devices, such as computers, Personal Digital Assistants (PDA) and mobile phones, over short distances using infrared signals.

**IT Security Zones** (Zones de sécurité des TI) – a networking environment with a well-defined boundary, a security authority and a standard level of susceptibility to network threats.

## K

**Key** (Clé) – a device to lock or unlock doors, cabinets, containers; includes metal keys and electronic access cards.

**Key Management** (Gestion des clés) - the procedures and mechanisms for generating, disseminating, replacing, storing, archiving, and destroying keys which control encryption or authentication processes.

**Key Material** (Matériel de chiffrement) - key, code, or authentication information that is in physical or electronic form.

**Key pair** (Biclé) - a pair of keys held by or for a person that includes a private key and a public key that are mathematically related to, but different from, each other.

**Key personnel** (Personnel clé) – is defined as individuals within a continuity management team that has a key role in the continuity and recovery process. Key personnel would have a good understanding of the critical service and what is required to restore the service.

**Keystroke loggers** (Enregistreurs de frappe) – is malware that records the keys struck on a keyboard in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

## L

**Law enforcement record check** (Vérification du dossier de police) - is a verification conducted by the RCMP within various databases containing police information.

**Lead** (Responsable) - the area/region requesting and/or developing an exercise (such as at the regional or branch levels) with or without the assistance of the headquarters Emergency Management Section of the Border Operations Centre and Major Events Directorate (for an AAR); or the area/region affected by an event/incident (at the regional or Branch levels) where normal operational procedures have been affected (for AER or AIR).

**Least privilege** (Privilège minimum) – determining and identifying the minimum system access permissions for each employee to perform their-work related duties following the principles of need-to-know and segregation of duties

**Life cycle** (Cycle de vie) – a series of stages through which a record passes during its lifetime. This includes the planning and needs analysis; creation, collection or receipt of records; organization, retrieval, use, accessibility, and transmission; storage and protection; and disposition.

**Likelihood** (Probabilité) – the number of instances that a particular outcome occurs within a set.

**Line authority** (Autorité hiérarchique) – the organization above an individual or part of the organization that determines the priority of work, assigns resources, monitors the performance of work and is accountable for varying degrees of service delivery. While an individual is directly accountable to his or her line manager, the determination regarding the appropriateness of work done is often determined as a result of the requirements of functional authorities within an organization.

**Local area network** (Réseau local) - is a computer network that interconnects computers in a limited area.

**Local element** (Élément local) - individual registered at a COMSEC Account or COMSEC Sub-Account who may receive COMSEC material from that account.

**Local security official** (Représentant local de la sécurité) - is an individual who has been assigned security responsibilities for the implementation of Agency security policies, standards and procedures.

**Locally-Accountable COMSEC Material** (Matériel COMSEC comptabilisé localement) - COMSEC material that has been assigned an Accounting Legend Code 4 or 7 and which is continuously accountable within a COMSEC Account after initial receipt has been sent to the distributing COMSEC Account.

**Loss** (Perte) – an article is "lost" when the owner no longer has possession or custody of it, involuntarily and by any means, but more particularly by accident or his own negligence or forgetfulness, and when he/she is ignorant of its whereabouts or cannot recover it by an ordinarily diligent search.

**Low degree of injury** (Faible prejudice) - Will generally result in such things as public embarrassment, minor financial loss, and inconvenience in conducting federal-provincial or international relations and minor disruption of internal government operations leading to delays and loss of information. The service supports the CBSA mandate, but the longer downtime is acceptable, as it can be interrupted without any significant impact.

# M

**Major tenant** (Locataire majoritaire) – federal tenant who occupies the majority of the space in a building.

**Malfeasance** (Délit d'action ou de commission) - Is the commission of an unlawful act whereby the perpetrator has no right to perform that act or is prohibited by contract, statute or regulation from performing that act.

**Malicious Code** (Code malveillant) – an element intended to design viruses, Trojan horses, worms and generally any program or code destined to create computer problems as opposed to solving them.

**Malicious email** (Courriel malveillant) - is defined as: a computer-based, electronic message containing file attachments or hyperlinks which if opened could cause the exploitation of the computer system and installation of harmful software.

**Malware** (Logiciels malveillants) – malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability. NOTE Viruses, worms, and Trojan horses, spyware and adware are examples of malware.

**Management of information technology security** (Gestion de la sécurité des technologies de l'information) - are security requirements that federal departments must fulfill to ensure the security of information and information technology (IT) assets under their control.

**Management practices and controls** (Pratiques et contrôles de gestion) - are policies, processes, procedures and systems that enable a department to operate its programs and activities, use its resources efficiently and effectively, exercise sound stewardship, fulfil its obligations and achieve its objectives.

**Manager** (Gestionnaire) - means an employee who acts in a supervisory role or managerial capacity and includes a Director.

**Managers at all levels** (Gestionnaires à tous les niveaux) — Includes supervisors, managers and executives.

**Master key** (Passe-partout) – a single key that operates locks that are keyed differently or alike, under the master key.

**Material** (Matériel) – any tangible object with the exclusion of those embodying information.

**Maximum Allowable Downtime** (Temps d'arrêt maximal admissible) – is the longest period of time for which a service can be unavailable or degraded before a medium of high degree of injury results. If a service needs to be continuous there would be a zero MAD.

**Medium degree of injury** (Préjudice moyen) - will generally result in such things as injury or illness to individuals, inability to conduct criminal investigations or other impediments to effective law enforcement, serious loss of public confidence, compromise of particularly sensitive personal information, significant financial loss or disruption to the economy, ineffectiveness in conducting international or federal-provincial relations, and disruption of services that would seriously inconvenience Canadians. The service, which if interrupted, could compromise the health, safety, security, or economic well-being of Canadians.

**Minimum safeguard** (Mesure de protection de base) – mandatory provisions of the Security Program, based on the Policy on Government Security, and its associated standards and technical requirements (see also Baseline Security Requirements).

**Minimum service level** (Niveau de services minimal) – the level of service delivery which is essential to avoid a high degree of injury; is maintained until full recovery is achieved.

**Minimum system access permissions** (Permissions d'accès minimal aux systèmes) - the need for someone to have only the required accesses to perform their duties.

**Misappropriation** (Détournement) - is the act of diverting money or property to a wrongful purpose. It is often used in the context of, but is not limited to, the diversion of public funds for one's own use or the use of others; however, any use not authorized by Parliament is a form of misappropriation.

**Misfeasance** (Faute d'exécution) - is the improper performance of a lawful act.

**Misuse** (Mauvaise utilisation) - any action or inaction by a user that is contrary to established policy, standards, procedures or practices of CBSA or that constitutes an unacceptable activity, an unlawful activity or a criminal activity.

**Misuse of CBSA e-mail system** (Mauvaise utilisation du système de courriel de l'ASFC) - use of the Agency e-mail system to conduct criminal, unlawful, and unacceptable activities.

**Misuse of credentials** (Mauvaise utilisation des justificatifs) - the use of any CBSA identification (including the CBSA badge) in a manner which may reasonably give the perception that it is being used for personal benefit, attempting to exert undue influence, or to obtain, directly or indirectly, a favour, reward, or preferential treatment for themselves or others, or to improperly enhance their own image.

**Misuse of duty firearm** (Mauvaise utilisation des armes de service) – non-compliance with policies, procedures or guidelines pertaining to the use of Agency firearms and defensive equipment.

**Misuse of government property** (Mauvaise utilisation des biens du gouvernement) - misuse of CBSA property includes the use of such property for purposes other than for official CBSA business. CBSA property includes, but is not restricted to, vehicles, buildings, space, premises, facilities, uniforms, files and documents, office equipment and supplies, computers, software, video equipment, telecommunication devices, government credit cards and defensive equipment.

**Misuse of IT systems** (Mauvaise utilisation des systèmes de TI) - noncompliance with policies, procedures or guidelines pertaining to information technology systems including, but not limited to, the use of e-mail, internet, file storage and access to CBSA and non-CBSA owned databases and the information they contain.

**Misuse of social network** (Mauvaise utilisation des réseaux sociaux) - use of social media tools in a way that compromises the Agency's reputation or working relationships with colleagues, stakeholders and clients.

**Mitigation** (Atténuation) – sustained actions taken to eliminate or reduce risks and impacts posed by hazards well before an incident or disaster occurs; mitigation activities may be included as part of prevention.

**Mobile broadband** (Services à large bande mobile) – is the name used to describe various types or wireless high-speed internet access through a portable modem, telephone or other device.

**Modification** (Modification) – the corruption or alteration of information, data, software or information systems equipment. Serious often because it is difficult to ascertain that corruption or alteration has taken place, especially in the machine readable environment.

**Monitor** (Surveillance) - monitoring is the continuous checking of network and system activity for abnormal, unlawful, inappropriate, criminal or unusual activity.

**Monitor versus screen access** (Surveillance contre contrôle d'accès) - monitor access provides a surveillance and security response to disturbances at the perimeter and common areas of a facility. Screen access - provides an identification and checking service on behalf of the tenant (for example, examining IDs, having persons sign-in upon entering the facility, etc.).

**Monitored** (Surveillé) – to watch for or detect a breach of security.

**Monitored continuously** (Surveillé continuellement) – to confirm on a continuous basis that there has not been a breach of security. Examples include electronic intrusion detection system, or someone guarding a particular point on a constant basis.

**Monitored periodically** (Surveillée sur une base périodique) - to confirm on a regular basis that there has not been a breach of security. The frequency and diligence of monitoring is based on the recommendations of a Threat and Risk Assessment. Examples include a guard patrol, or employees working at the location.

**Monitoring (IT)** (Surveillance (TI) - the continuous checking of network and system activity for abnormal, unlawful, inappropriate, criminal or unusual activity.

**Monitoring (Physical)** – (Surveillance) The process of checking, observing or validating the accounting of assets at specified intervals.

**Monitoring of electronic resources** (Surveillance des ressources électroniques) - the recording and analysis of the use of electronic resources for operational purposes and for assessing compliance with government policy.

**Monitoring of e-mail** (Surveillance des courriels) - any action that involves the recording and subsequent analysis of activity or use of services as defined in this policy and the CBSA Policy on the Use of Electronic Resources.

**Multi-institutional privacy impact assessments** (Évaluations multi-institutionnelles des facteurs relatifs à la vie privée) - is a privacy impact assessment that involves more than one government institution. (See definition of privacy impact assessment)

## N

**National COMSEC Incidents Office** (Bureau national des incidents COMSEC) - the entity at Communications Security Establishment Canada responsible for managing COMSEC incidents through registration, investigation, assessment, evaluation, and closure.

**National interest** (Intérêt national) - Concerns the defence and maintenance of the social, political and economic stability of Canada and thereby the security of the Nation. Information that might injure the National Interest if compromised is defined by specific sections of the Access to Information Act and the Privacy Act as described in article 2.1 of the Security Policy.

**Natural** (Naturel) – as provided by various Emergency management databases, weather services, the World Health Organization and travel organizations (specifically flora and fauna).

**Need to Know** (Besoin de connaître) – the need for someone to access and know information in order to perform his or her duties. Access to facilities, systems and information is limited to those with a "need-to-know". This means it is limited to users with the appropriate security screening level, and that users only have access to information and systems that are required to fulfill their duties.

**Neglect of Duty** (Manquement au devoir) - failure to follow applicable laws, rules, policies, orders of superiors in the performance of duty.

**Negligence** (Négligence) - is causing loss of money or damage to property as a result of doing something or failing to provide a proper or reasonable level of care.

**Network** (Réseau) – a computer network can be local, or extended. It allows transmission in digital format of all types of data, which can be used by the entire network.

**Non critical security incident** (Incident de sécurité non critique) - is of a lesser magnitude than a critical security incident however may impact border operations. These security incidents require timely reporting.

**Non-administrative purpose** (Fins non-administratives) - is the use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistical, audit and evaluation purposes.

**Nonfeasance** (Omission délictueuse) - is the omission of or failure to perform some specific act, duty or undertaking that one is obliged to do.

**Non-repudiation** (Non-répudiation) – non-repudiation services provide a user with protection against another user later denying that some communications exchange took place. In general, the non-repudiation evidence must prove convincing to a third party arbitrator.

**Non-sensitive** (De nature non délicate) - assets which are neither protected nor classified.

**Nudity** (Nudité) - is a naked person or a person displaying genitalia. Does not need to be sexual in content.

# O

**Observation** (Observation) - an issue that was observed during the exercise/event/incident.

**Observer (for EM or BCM exercises)** (Observateur pour MU ou exercices PCA) - participants who are neither players nor trusted agents. Observers witness exercise events.

**Observer (for Professional Standard Investigations)** (Observateur Enquêtes relatives aux normes professionnelles) means a person who is an employee that is neither a witness in the Professional Standards investigation nor acting in their capacity as a union representative, invited by the respondent and permitted by the investigator to sit in during an interview of the respondent by the investigator.

**Occupation** (Occupation) – when a group or individuals occupy premises and refuse to leave as a means of expressing views and exercising political pressure.

**Offensive material** (Matériel à contenu offensant) - is likely to insult, disgust or repulse. These include jokes made against select groups (e.g., racial, religious, or sexist jokes). It may also include offensive images (e.g., images of corpses, portrayals of defecation).

**Official records** (Documents officielles) – are records with business value that provide evidence of the conduct of government business and decision-making such as planning documents, meeting documents, financial records, etc.

**Open source** (Source générale) - refers to information and data available to the general public that do not require a user id and/or password to obtain access.

**Operations zone** (Zone de travail) – is an area where access is limited to personnel who work there and to properly escorted visitors; it must be indicated by a recognizable perimeter and monitored periodically. Example – typical open office space.

**Opportunity for improvement** (Possibilité d'amélioration) – a failure to meet the requirements associated with a security control that does NOT expose an asset directly to the potential for compromise.

**Orientation seminar** (Séminaire d'orientation) - a discussion-based exercise used to provide information and introduce people to policies, plans and procedures. It is a low-stress, information discussion in a group setting with little or no simulation.

**Other Information** (Autres renseignements) - The term used to describe the mass of government information that qualifies neither for classification in the National Interest nor for protection as other sensitive information.

## P

**Pandemics (**Pandémie) – an epidemic of infectious disease that has spread through human populations across a large region; for instance multiple continents, or even worldwide.

**Password** (Mot de passe) – it is a string of characters (ie. letters, numbers and other symbols) used to authenticate an identity or to verify access authorisation. It is used in combination with a user name to access a workstation, an application, an on-line service or a network server.

**Perimeter** (Périmètre) – exterior limit of a site.

**Personal electronic device** (Dispositif électronique personnel) - any electronic device that is owned by the employee (e.g. Cellphones, Smartphones (iPhones, Blackberry's, etc.), iPods, MP3 players, Digital Cameras, Bluetooth devices, Laptops, etc.)

**Personal equipment** (Matériel personnel) – assets that are the property of employees. (i.e. employee's cash, coffee fund, clothing or other personal items) *although loss or theft of personal equipment is not a CBSA responsibility, it could indicate a security problem within the office. Report incidents to your local security.

**Personal information** (Renseignements personnels) - information recorded in any form about an identifiable individual. This includes, but is not limited to, the following types of information about an individual: race, age and marital status; education; medical, criminal, financial and employment history; any identifying number assigned to the individual; fingerprints; address; personal views; and so on.

**Personnel security** (Sécurité personnelle) - refers to the maintenance of the appropriate standards of conduct, and the review of the reliability and assessment of loyalty to determine the level of security screening (i.e. reliability, secret and top secret) for all persons given access to the Agency infrastructure (facilities, assets, information, systems, etc.).

**Personnel security clearance** (Attestation de sécurité du personnel) – the process to ensure that those who have access to government information, assets and services are honest, trustworthy, reliable and loyal to Canada.

**Personnel security screening** (Enquêtes de securité sur le personnel) – the process of examining the trustworthiness and suitability of employees and, where national interest is concerned, their loyalty and associated reliability; when satisfactory, an employee is granted reliability status or a security clearance. Reliability status applies when only protected assets are concerned. When the employee has access to classified assets, a security clearance corresponding to the level of classified assets is issued. A security clearance includes reliability status.

**Persons requiring assistance** (Personnes ayant besoin d'aide) – are individuals who cannot safely evacuate the premises on their own due to a permanent or temporary injury, illness, disability or medical condition. These individuals should self-identify with their manager/supervisor and with the Building Emergency Organization.

**Pharming** (Détournement de domaine) – is a common type of online fraud. A means to point you to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website.

**Phishing** (Hameçonnage) - a form of Internet fraud that uses authentic-looking but false e-mails, web sites or other information to steal valuable information such as credit cards, social insurance numbers, user IDs and passwords.

**Physical abuse** (Abus physique) – including assault, is the intentional use of force against a person without that person's consent. It can cause physical pain or injury that may last a long time.

**Physical safeguard** (Mesure de protection physique) - refers to the facilities and equipment that protects the support system in which personal information is recorded and stored.

**Physical security** (Sécurité matérielle) – the use of physical safeguards to prevent or delay unauthorized access to assets, to detect attempted and actual unauthorized access and to activate appropriate responses.

**Physical security equipment** (Équipement de sécurité matérielle) - those pieces of equipment, installations and building components designed or used to physically deny or control access to classified assets of Government; e.g. locks, containers, alarm systems, barriers and classified waste destruction equipment. It includes those ancillary systems which are vital to the proper operation of those pieces of equipment, installations and building components.

**Piggybacking** (Passage en double) – refers to when an individual tags along or follows an authorized employee through a security checkpoint or doorway without being processed through the system. The act is unacceptable and may be legal or illegal, authorized or unauthorized, depending on the circumstances.

**Platform** (Plate-forme) – a computer, including the hardware, operating system and associated infrastructure, attached to a computer network that processes, collects, transmits or stores information.

**Platforms owner** (Propriétaire de plates-formes) - those responsible for defining the IT computing environment, infrastructure service support, and security requirements for their respective platform. Platform owners may delegate to asset owners the responsibility of administering the access on a day-to-day basis.

**Players** (Intervenants) - exercise participants who perform or discuss their assigned roles and functions in exercise situations using their normal response procedures (unless directed otherwise). They react to information provided by other players and simulators and initiate actions to manage and mitigate the simulated emergencies.

**Policy on government security** (Politique sur la sécurité du government) - a policy that helps protect the Government of Canada's personnel and assets; it outlines vital safeguards for reducing risks of injury from various threats.

**Pornography** (Pornographie) - is explicitly sexual material designed or intended to cause sexual arousal or titillation.

**Preliminary inquiry** (Pré-enquête) – the act of obtaining from the person who made the allegations all details relating to the facts and circumstances reported, examining the documentation available in order to determine whether the allegation may warrant formal investigation.

**Preparedness** (Préparation) – a phase of emergency management consisting in making decisions and taking measures prior to an emergency, in order to be ready to effectively respond to it and manage its consequences.

**Pretexting** (Faux-semblant) - is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.

**Prevention** (Prévention) - physical, procedural, technical or administrative controls that are intended to ensure that the individuals, assets, or operation are protected from harm to the extent possible.

**Primary systems** (Systèmes primaires) - are databases such as CAS, mainframe applications and network applications. They are provided for Agency business purposes only.

**Principle of Least Privilege** (Droit d'accès minimal) - a basic principle that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

**Privacy** (Vie privée) - is the right of an individual to be left alone, to be free of unwarranted intrusions. It is also the right of an individual to retain control over his or her personal information and to know the uses, disclosures and whereabouts of that information.

**Privacy Act** (Loi sur la protection des renseignements personnels) – protects the privacy of individuals by setting requirements for collection, use, retention or disposal of personal information in the federal government. Security plays an essential role in the protection of personal information from unauthorized disclosure or use.

**Privacy breach** (Atteinte à la vie privée) - involves improper or unauthorized creation, collection, use, disclosure, retention or disposal of personal information.

**Privacy impact assessment** (Évaluations des facteurs relatifs à la vie privée) – a policy process for identifying, assessing and mitigating privacy risks. Government institutions are to develop and maintain privacy impact assessments for all new or modified programs and activities that involve the use of personal information for an administrative purpose

**Privacy notice** (Avis de confidentialité) - is a statement presented to an individual to communicate the purpose of a collection, including the authority of the government institution to collect, use and disclose the personal information for a given program or activity. It also states the rights of individuals to access their own personal information kept in the program's PIB and the consequences for refusing to provide their personal information.

**Privacy practices** (Pratiques relatives à la protection de la vie privée) - refers to all practices related to the creation, collection, retention, accuracy, use, disclosure and disposition of personal information.

**Privacy protocol** (Protocol relatif à la protection des renseignements personnels) - is a set of documented procedures to be followed when using personal information for non-administrative purposes including research, statistical, audit and evaluation purposes. These procedures are to ensure that the individual's personal information is handled in a manner that is consistent with the principles of the Act.

**Privacy request** (Demande de renseignements personnels) - is a request for access to personal information under the Privacy Act.

**Private business** (Activité personnelle) - is an activity outside the scope of employment conducted for personal gain or profit. This includes the sale or purchase of any goods or services. This category also includes the conduct of political activity.

**Private key** (Clé privée) - a string of data that is used in asymmetric cryptography to encrypt data contained in an electronic document; and is unique to the person who is identified in, or can be identified through, a digital signature certificate and corresponds only to the public key in that certificate.

**Privileged Access** (Accès privilégié) - An authorization or set of authorizations that allows users to bypass logical access controls and execute functions that are normally forbidden to ordinary (non-privileged) users.

**Privileged system access permissions** (Permissions d'accès privilégié aux systèmes) - authorization or set of authorizations that allows users to bypass logical access controls and execute functions that are normally forbidden to ordinary (non-privileged) users.

**Privileged user** (Utilisateurs privilégiés) – users who, by virtue of function or role, have been allocated powers within an information technology system, which are greater than those available to the majority of users. There are three categories of privileged users: 1) support staff and administration of IT systems; 2) staff development of systems; 3) other personnel administration and security.

**Privileged user risk management (PURM)** (Coordonnateur de la Gestion de risques des utilisateurs privilégiés) - All privileged system access permissions are to be granted and removed through the Privileged User Risk Management (PURM) program and are valid for a defined period of time.

**Privileged user risk management system** (Système de gestion des risques des utilisateurs privilégiés) - on-line tool that manages workflow of PURM requests from the original requestor (applicant), management authorization (supervisor and Management Level 3 (ML3)), PURM coordinators, various administrators (platform/asset owners) and security areas where required, while keeping all stakeholders informed of the status of the request.

**Probability** (Probabilité) – a measure of the frequency or likelihood of an event.

**Profanity** (Blasphème) - includes material where vulgar (offensive) language is used. It includes, but is not limited to, vulgar language in a written text, oral use of the words in a sound file or video, or even a caption with an image.

**Professional Integrity** (Intégrité professionnelle) - employees are responsible for exercising their authority in an honest, open and fair manner; accepting responsibility for their actions in order to build and maintain a reputation of trustworthiness and accountability; treating others in a respectful manner; doing what is right even when nobody is looking; and safeguarding the physical and informational assets of the CBSA.

**Professional Standards Investigation** (Enquête des normes professionnelles) - means the formal investigation by a PSI investigator in accordance with the Guidelines for the Report, Review and Professional Standards Investigation of Alleged or Suspected Employee Misconduct

**Program or activity** (Programme ou activité) - is, for the purposes of the appropriate collection, use or disclosure of personal information by government institutions subject to this policy, a program or activity that is authorized or approved by Parliament. Parliamentary authority is usually contained in an Act of Parliament or subsequent Regulations. Parliamentary authority can also be in the form of approval of expenditures proposed in the Estimates and as authorized by an appropriation Act. Also included in this definition are any activities conducted as part of the administration of the program.

**Prohibited usage** (Utilisation interdite) - may include criminal offences, contraventions of non-criminal regulatory federal and provincial statues, and actions that make an authorized individuals or an institution liable to a civil lawsuit. Also, these activities may expose the department's network to malicious attack and exploitation.

**Protected** (Protégé) – the category which indicates that the information qualifies as other sensitive information and requires enhanced protection.

**Protected assets** (Biens protégés) – assets or information that may qualify for an exemption or exclusion under the Access to Information Act or the Privacy Act because unauthorized access/disclosure would reasonably be expected to cause injury to an individual or an organisation.

**Protected disclosure** (Divulgation protégée) - a disclosure that is made in good faith and that is made by a public servant:

(a) in accordance with this Act (Public Servants Disclosure Protection Act);

(b) in the course of a parliamentary proceeding;

(c) in the course of a procedure established under any other Act of Parliament; or

(d) when lawfully required to do so.

**Protected information** (Renseignement protégé) – information related to private, business and other non-national interest that may qualify for an exemption or exclusion under the Access to Information

Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to an individual or an organisation.

- Protected A (Protégé A): Minor injury if compromised. Unauthorized release could cause injury to an individual, organization or government (e.g. loss of privacy, embarrassment, etc.)
- Protected B (Protégé B): Medium to Serious Injury if compromised. Unauthorized release could cause serious injury to an individual, organization or government (e.g. prejudicial treatment, loss of reputation or competitive edge, etc.)
- Protected C (Protégé C): Unauthorized release could cause extremely grave injury to an individual, organization or government (e.g. significant financial loss, loss of life, Witness Protection Program, informant information, etc.).

**Protection** (Protection) – for physical security, protection means the use of physical, procedural and psychological barriers to delay or deter unauthorized access, including visual and acoustic barriers.

**Provision** (Disposition) – the process of coordinating the creation of user accounts and access permissions to those accounts.

**Psychological ethical testing** (Examen éthique et psychologique) - for employees and new recruits to evaluate psychological readiness to carry a firearm safely and responsibly for the Canada Border Services Agency (CBSA).

**Public funds** (Fonds publics) – for physical security, protection means the use of physical, procedural and psychological barriers to delay or deter unauthorized access, including visual and acoustic barriers, money funded in government securities or through the levy of taxes from a governmental entity (i.e. petty cash, funds within a cashier operation or while in transit).

**Public information** (Renseignements publics) - the public category recognizes that the information lies outside the national interest, is non-sensitive (non-protected and non-classified) and does not have a degree of potential injury, and therefore does not require any protective measures.

**Public key** (Clé publique) - a string of data contained in a digital signature certificate that (a) is used in asymmetric cryptography to decrypt data contained in an electronic document that was encrypted through the application of the private key in the key pair; and (b) corresponds only to the private key in the key pair.

**Public key certificate** (Certificat de clé publique) - the public key information of an entity signed by an appropriate certification authority and thereby rendered unforgivable.

**Public key infrastructure PKI** (Infrastructure à clé publique ICP) - is a dual encryption system which ensures security in electronic transactions, and also confirms that the person who sends an electronic record is who they appear to be, and that the electronic record sent by them has not been tampered with by anyone else. PKI adopts methods for using a secure electronic signature to ensure the validity and integrity of electronic records. It also includes a system of digital certificates, Certificate Authorities

and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

**Public money** (Fonds publics) - is all money belonging to Canada received and collected by the Receiver General or any other public officer in his or her official capacity or any person authorized to receive or collect such money.

- Duties and revenues of Canada;
- Money borrowed by Canada or received through the issue or sale of securities;
- Money received or collected for or on behalf of Canada; and
- All money that is paid to or received or collected by a public officer under or pursuant to any act, trust, treaty, undertaking or contract, and is to be disbursed for a purpose specified in or pursuant to that act, trust, treaty, undertaking or contract.

**Public property** (Biens publics) - is all property (including data), other than public money, belonging to Her Majesty in Right of Canada.

**Public Zone** (Zone d'accès public) – the area surrounding a government facility to which the general public has access.  One should never handle sensitive information in public zones.

**Public-access zone** (Zone d'accès public) - generally surrounds or forms part of a government facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple occupancy buildings.

**Pyramid schemes** (Opérations pyramidales) - are hierarchies in which you are encouraged to send money with the expectation that a set number of individuals will in turn send you money.

**Quid pro quo** (En contrepartie de) - means something for something. For instance an attacker calls random numbers at a company, claiming to be calling back from technical support. Eventually this person will hit someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker access or launch malware.

## R

**Readiness exercises and disaster simulation** (Exercices de préparation et de simulation de sinistre) – is a mechanism through which the Agency can test and validate its emergency management plans and emergency communication frameworks in preparation of an emergency.

**Readiness levels** (Niveaux de préparation) — Levels of heightened security that are to be applied within government facilities in Canada in times of emergency or increased threat situations.

**Reception zone** (Zone d'accueil) – the transitional area from a public zone to an operations zone. Generally located at the entrance of a facility, this zone offers the first physical security challenge to the public by employing security measures such as doors and other physical barriers (turnstiles). Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the Reception Zone is indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment. Departmental assets or information must never be stored or left unattended in this type of zone.

**Recommendation** (Recommandation) - a recommended course of action that can either perpetuate a positive finding, or address an area for improvement.

**Reconciliation** (Rapprochement) - the process of comparing two or more sets of data to resolve discrepancies and demonstrate proof of accuracy.

**Record** (Document) – any documentary material other than a publication, regardless of medium or form. Records are information created, received and maintained by an organization or person for business purposes, legal obligations, or both. A "record" also includes a sound recording, videotape, film, photograph, chart, graph, map, plan, and survey, data. Furthermore this also includes all originals, copies and drafts of the same record.

**Recover** (Reprise) - Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster.

**Recovery** (Rétablissement) - Actions taken to repair or restore conditions to an acceptable level after a disaster.

**Recovery point objective** (Objectif de point de rétablissement) - the point in time to which data must be recovered in order to be acceptable to the owner of the processes supported by that data.

**Recovery time objective** (Objectif de délai de rétablissement) - the period of time within which systems, applications and infrastructure must be recovered after a disaster.

**Regional Security Manager** (Gestionnaire régionaux de la sécurité) - is an individual who has been assigned security responsibilities for the delivery of security policies, procedures, guidelines in one of the regions

**Registered mail** (Courrier recommandé) - a postal mailing term/service for letter-mail only provided by Canada Post or equivalent service abroad which provides the sender with proof of mailing and/or proof of delivery. This service provides the sender with a mailing receipt and secures the signature of the addressee, a print of the signature and the date upon delivery's, standards and procedures in a region.

**Regulatory impact analysis** (Étude d'impact de la réglementation) - is a tool used for regulatory reform, which assesses the impact of regulation on the quality of the environment and the health, safety, security, and social and economic well-being of Canadians.

**Relative** (Parenté) – any person who is a member of a class of persons connected by blood, marriage or common-law relation, or by adoption or other legal bond.

**Relevant** (Pertinent) – clearly connected or appropriate to the matter at hand.

**Reliability status** (Cote de fiabilité) – a CBSA Reliability Status is the type of screening required when the duties or tasks of a position or contract necessitate access to designated information and assets. An individual granted Reliability Status may access, on a need-to-know basis, designated information and assets. A CBSA Reliability Status forms the basis required for a Secret or Top Secret clearance.

**Reliable source** (Source fiable) - is a source of information or a data holding deemed to be accurate and up to date and, as such, can be trusted and relied on for the purposes of validating personal information.

**Removable media** (Support amovible) – medium which can be used as secondary or extended memory for a computer but which can also be conveniently removed and used as a storage device. Examples of removable media are USB memory sticks, CDs/DVDs and external hard drives.

**Removable media storage devices** (Dispositive de stockage amovible) – the storage of media is designed to be removed from the computer with powering off the computer. Some types of removable media are designed to be read by readers and drives such as optical disks (CD's, DVD's) or memory cards. Removable media may also refer to some removable storage devices, when they are used to transport or store data, such as USB flash drives or external hard disk drives.

**Reporting life cycle** (Déclaration du cycle de vie) - an Operations Branch framework used by the Emergency Management Section to ensure that recommendations made following exercises, events or incidents are prioritized for action.

**Reprisal** (Représailles) - any measures taken against a public servant because he/she has made a protected disclosure or has, in good faith, cooperated in an investigation into a disclosure or an investigation commenced under section 33 (of the Public Servants Disclosure Protection Act).

**Request management** (Gestion des demandes) - the processes by which the business community interacts with those that provide the services. Request Management is a process discipline for managing any request from enabling its initial submission, providing authorization and orchestrating its fulfillment.

**Residual Risk** (Risque résiduel) — Level of risk remaining after taking into consideration risk mitigation measures and controls in place.

**Resilience** (Résilience) – the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure.

**Respondent** (Intimé) – means an employee against whom a complaint is made.

**Response - emergency management** (Intervention – gestion d'urgence) – actions taken during or immediately before or after a disaster to manage its consequences and minimize suffering and loss.

**Response** (Réponse) - the reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required; addressing matters of life safety and evacuation. Response also addresses the policies, procedures and actions to be followed in the event of an emergency.

**Response IT** (Incident response or intrusion response) (Intervention en TI (intervention en cas d'incident ou d'intrusion) - actions taken to protect and restore the normal operational conditions of an information system and the information stored in them when an attack or intrusion occurs.

**Response plan** (Plan d'intervention) – an emergency plan that describes actions and procedures that apply to the response phase of an event.

**Responsible Building Authority** (RBA) (Autorité responsable de l'immeuble) - Where the CBSA is the only tenant or the facility is shared with the private sector, the RBA is defined as the most senior CBSA official. Where the CBSA is located in a multi-tenant, federal facility environment, the most senior official of the major "government" tenant is considered to be the RBA.

**Restricted access area** (Zone d'accès restreint) – work areas where access is limited to authorized individuals. It includes Operations, Security and High-Security Zones.

**Restricted zone** (Zones restraintes) - includes Operations, Security and High Security Zones. Refer to definition of "Zones".

**Review for cause** (Examen justifié) – a review for cause is a reassessment of an individual's eligibility to hold a security screening level previously granted. It is a formal process that is initiated when new information is uncovered or reported about an individual that may call into question their reliability and/or loyalty.

**Risk** (Risque) –the chance of a vulnerability being exploited. Within the context of the TBS, risk is also defined as "the uncertainty that can create exposure to undesired future events and outcomes. It is an expression of the likelihood and impact of an event with the potential to impede the achievement of an organization's objectives.

**Risk analysis / Evaluation** (Évaluation/analyse du risque) - The systematic analysis of the conditions, actions and their interaction that make up a particular risk.

**Risk assessment** (Évaluation des risques) – an evaluation of the chance of vulnerabilities being exploited based on the effectiveness of existing or proposed security measures.

**Risk criteria** (Critères de risqué) – Terms of reference by which the significance of risk is defined and assessed by a department to determine whether it is acceptable or unacceptable.

**Risk informed approach** (Démarche de prise en compte du risque) – To management builds risk management into existing governance and organizational structures, including business planning, decision-making and operational processes. It also ensures that the workplace has the capacity and tools to be innovative while protecting the public interest and maintaining public trust.

**Risk inventory** (Inventaire des risques) - the process of detecting, recognizing and recording risks.

**Risk management** (Gestion du risque) – a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.

**Risk mitigation** (Atténuation du risque) - is the processes built into the controls environment, such as policies, frameworks, accountabilities etc. to lower the residual risk (remaining risk lowered to an acceptable level).

**Risk response** (Réaction aux risques) - refers to the continuum of measures of risk mitigation or control that are developed and implemented to address an identified risk.

**Risk tolerance** (Tolérance au risque) - is the willingness of an organization to accept or reject a given level of residual risk (exposure). Risk tolerance may differ across the organization, but must be clearly understood by the individuals making risk-related decisions on a given issue. Clarity on risk tolerance at all levels of the organization is necessary to support risk-informed decision-making and foster risk-informed approaches.

**Robbery** (Vol qualifié) - Is the taking of money, property, or any other article of value against a person's will through violence or threat of violence.

**Role based access guides** (Guides d’accès fondés sur les rôles) - the authoritative source for assigning minimum system access permissions.

**Rootkit** (Rootkit) – is a stealthy type of malware designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

# S

**Safeguarding strategy** (Stratégie de mesures de protection) – security measures identified as a result of a threat and risk assessment to safeguard employees, information and other assets.

**Safeguards** (Mesures de protection) – approved and implemented to ensure the confidentiality, integrity, availability and authenticity of information and protection of employees and assets. These are normally identified through a risk management process.

**Sanitized** (Nettoyer) - to purge data of personally-identifiable information in order to protect user privacy.

**Screening** (Filtrage) – the process of verifying visitors and/or material at entry points of a facility or a restricted area for authorizing access.

Secondary systems (Systèmes secondaires) – secondary systems are comprised of applications such as e-mail, Microsoft Office and Internet (where limited personal use is permitted).

**Secret Information** (Renseignement secret) - unauthorized release could cause serious injury to the national interest. Examples include minutes or records of Cabinet, committees, draft legislation, strategies, tactics relating to international negotiations, case files with national security implications.

**Secure** (Sécurisé) – the condition that arises when an organization is operating at or below an acceptable level of residual risk that has been arrived at through the application of sound practices fairly and consistently applied.

**Secure classified facsimile network** (Réseau de télécopieurs classifiés) - refers to special facsimiles attached to an approve encryption device for the transmission of up to Top secret data.

**Secure file transfer** (Transfert sécurisé de dossiers) - files containing sensitive information such as partner data are encrypted using off-line CRA-approved encryption to protect the confidentiality of the file or files. This method ensures that files are protected and suitable for transfer across an unencrypted network link. Off-line encryption is the responsibility of the end-user.

**Secure network** – (Réseau sécurisé) - a secure network verifies the authenticity of all network endpoints and protects the confidentiality of data being transmitted between endpoints. Confidentiality controls can include bulk encryption of session traffic (e.g. Secure Sockets Layer), network traffic (e.g. IPSec), or links between sites using CBSA-approved encryption. This method permits files to be transmitted between network endpoints without additional off-line encryption tasks.

**Secure protected facsimile network** (Réseau de télécopieurs protégés) - refers to facsimiles attached to approve encryption device for the transmission of up to Protected B data.

**Secure room** (Pièce sécuritaire) - a totally enclosed space having features of physical security which protect assets stored within it against specific threats.

**Security administration and program coordination** (Administration de la sécurité et coordination du programme) - refers to the documentation of policies, standards, guidelines, procedures and baselines regarding internal security requirements and the establishment of appropriate mechanisms associated with agreements involving assets or risks being shared across organizations.

**Security advisor** (Conseiller en sécurité) – is a member of the local security office who provides security advice and support as it relates to emergency response activities; the security advisor must not hold specific responsibilities as a member of the building emergency organization.

**Security assessment** (Évaluation de sécurité) — In accordance with section 2 of the CSIS Act, an appraisal of an individual's loyalty to Canada and, so far as it relates thereto, his/her reliability.

**Security awareness** (Sensibilisation à la sécurité) - refers to those practices, technologies and/or services used to promote user awareness, user training, and user responsibility with regard to security risks, vulnerabilities, methods, and procedures related to information technology resources.

**Security breach** (Infraction à la sécurité) - An act or omission, deliberate or accidental, that results in the actual or possible compromise of controlled goods (as defined in Part 2 of the Defence Production Act) or related technology; such breaches may include controlled goods or technology lost while being transported; controlled goods or technology left in an unsecured area where unauthorized persons have access; unauthorized disclosure by any person; theft; and loss, or exposure in circumstances that make it probable that a breach has occurred.

**Security Clearance** (cote de sécurité) - indicates successful completion of a security assessment; with a need to know, allows access to classified information. There are three Security Clearance levels: Confidential, Secret and Top Secret.

**Security container** (Coffre de sécurité) – any totally enclosed storage place for a classified asset, designed to resist force and surreptitious attacks; e.g. a safe, security cabinet, strongbox, permanent vault, demountable vault or secure room.

**Security control** (Contrôle de sécurité) – an administrative, operational, technical, physical or legal measure for managing security risk. This term is synonymous with safeguard.

**Security control objective** (Objectif des contrôles de sécurité) – a security control objective can be described as statements of desired results or purposes to be achieved by implementing controls

**Security controlled asset management** (Gestion des biens de sécurité contrôlés) - is a system of internal control processes through which the CBSA is provided with reasonable assurance that the following are achieved: proper control and accounting of controlled assets; reliable tracking and reporting through the lifecycle of the assets; and compliance with applicable Canadian laws, regulations and policies prescribing requirements to ensure control of the assets.

**Security Control Form** (Formulaire de contrôle) - The Security Control Forms are the forms used to track all movements of the Security Controlled Asset as well as all incidents pertaining to the Security Controlled Asset.

BSF208: Controlled Asset Form

BSF203:  Status Designation CBSA Port Stamp – Sample Impressions

BSF152: Security Incident Report

BSF270: Custodian Departure/Transfer Notification

BSF672: Daily Port Stamp Allocation

**Security Control Objective** (Objectif des contrôles de sécurité) – These are described in Appendix C of the Directive on Departmental Security Management as published by the Treasury Board of Canada Secretariat (TBS). A security control objective can be described as statements of desired results or purposes to be achieved by implementing controls (adapted from COBIT).

**Security design brief** (Guide de sécurité de la conception) – describes the physical protection philosophy and concepts as well as physical safeguards required for a facility.

**Security function** (Function de sécurité) — An activity that directly supports the achievement of government security objectives, including activities related to security awareness and training, security screening of individuals, physical security (including prevention of violence in the work place), information and information technology security, security in contractual and non-contractual arrangements, security incident management, identity management and business continuity planning, and overall management of security in a department or agency, or government-wide.

**Security goals** (Objectfs de sécurité)– security goals are those conditions that arise when the security control objectives function as anticipated in maintaining an appropriately determined level of residual risk.

**Security guidelines** (Ligne de conduite) – suggested methods based on best practices to implement Agency security policies, standards and procedures.

**Security incident** (Incident de sécurité) – any workplace violence toward an employee or any act, event or omission that could result in the compromise of information, assets or services. PGS

- Critical Security Incident (Incident de sécurité critique) - a critical security incident has the potential to seriously affect the overall functions of the CBSA by causing serious injury or loss of life, significant property damage, threat to services/operations and/or partial or complete disruption of border operations. Immediate action (reporting) is necessary to mitigate the impact of these security incidents.
- Non Critical Security incident (Incident de sécurité non critique) - is of a lesser magnitude than a critical security incident however may impact border operations. These security incidents require timely reporting.

**Security Incident** (incident de sécurité) - An activity involving such matters as theft/loss of revenue, money or assets; unauthorized accesses to, loss of and/or disclosure of client or other classified and/or

protected information; violations by employees of the Criminal Code or other Federal Statutes and certain administrative policies administered by the CBSA; threats of harm by members of the public made against the CBSA and its employees; and, any other similar situation such as occupations, which could be of interest to the media or the subject of adverse publicity.

**Security incident reporting** (Signalement des incidents de sécurité) - involves the identification, investigation, reporting, processing and analysis of events associated with security breaches, the loss or damage to assets, of confidentiality, integrity and/or, availability, and relative value or public confidence in the Agency's employees, sensitive assets or operations.

**Security inspection** (Inspection de sécurité) – a formal review of the implementation of security policies, standards, and procedures.

**Security manual** (CBSA) (Manuel de sécurité )- is a series of policies and standard operating procedures that support the implementation of the Policy on Government Security (PGS) issued by the Treasury Board Secretariat (TBS).

**Security of Information Act** (Loi sur la protection de l'information) - identifies penalties for conduct related to information security, such as espionage, that is or is likely to be harmful to Canada.

**Security Marking(s)** (Mention(s) de sécurité) – Consistent and accepted markings or metadata that are applied to information or assets in order to communicate the category and degree of sensitivity of that asset.

**Security official** (Responsable de la sécurité) – individual who has been assigned security responsibilities for the implementation of agency security policies, standards and procedures.

**Security policy** (Politique de sécurité) – stipulates mandatory Agency security requirements based on the Policy on Government Security. They are rules, directives and practices that ensure the protection of personnel, information and assets.

**Security practitioners** (Praticiens de la sécurité) - are defined as persons responsible for coordinating, managing and providing advice and services related to the security activities that are part of a coordinated departmental security program, which include but are not limited to information technology (IT) security, physical security, personnel security screening, emergency management, business continuity planning and regional security operations.

**Security program** (Programme de sécurité) – a group of security-related resource inputs and activities that are managed to address a specific need or needs and to achieve intended results.

**Security Requirement Check List** (Liste de verification relative à la sécurité) - form designed for use by Project Authorities, Departmental Security Officers, Procurement Officers or other government employees in the contracting process to identify security requirements at the start of any contractual or pre-contractual process.

**Security review** (Revue de sécurité) – a local evaluation of the implementation of Agency security policies, standards, and procedures.

**Security risk management** (Gestion du risque de securité) - is a systematic approach to assessing threats, analyzing risks and implementing controls. The key steps in the process include the identification, assessment, evaluation and treatment of security risks.

**Security screening** (Filtrage de sécurité) - The process of conducting a security screening activity and evaluating an individual's reliability and/or loyalty to Canada in support of a decision to grant, grant with a waiver, deny, or revoke a reliability status, security clearance or site access clearance.

**Security services** (Services de sécurité) — A service that fulfils or directly supports a security function; does not include general administrative services.

**Security site brief** (Guide de sécurité du site) - a document which describes the physical security attributes sought in a site when relocating the facility.

**Security standards** (Normes de sécurité) – detailed mandatory security requirements (deriving from security policies) developed by the Security and Professional Standards Directorate.

**Security sweep** (Ratissage de sécurité) - is the least formal of the monitoring activities that focuses on assessing compliance with security standards. Sweeps involve the periodic monitoring of the security posture within an organizational area and seek to ensure an acceptable level of security is being maintained.

**Security violation** (Atteinte à la sécurité) – any act or omission that results in an individual or entity attempting to bypass, avoid or remove a security control or otherwise reduce its effectiveness. It should be clear that security violations may come in many forms or various levels of gravity.

**Security Zone** (Zone de sécurité) - an area where access is limited to authorized personnel and authorized and properly-escorted visitors only. Protected C, Secret and Top Secret information can be handled within a security zone but it must be locked in an approved cabinet or safe; must be monitored 24/7.

**Segregation of duties** (Séparation des tâches) - segregation of duties refers to a process that is divided between different individuals in order to reduce the scope for error and fraud.

**Sensitive Assets** (Bien de nature délicate) - assets that warrant additional protection due to their value or the harm that would be caused by the destruction, removal, modification, interruption, loss, misuse, unauthorized access or disclosure.

**Sensitive information** (Renseignement de nature delicate) - information that must be protected because its disclosure, modification, loss, or destruction would reasonably be expected to cause injury to a non-national (protected) interest or a national (classified) interest.

**Sensitive misdirected correspondence** (Correspondance mal acheminée de nature sensible) - sensitive misdirected correspondence incidents involve a threat of media attention, a high profile disclosure, or a refusal to return the correspondence

**Service** (Service) - Provision of a specific final output that addresses one or more needs of an intended recipient and contributes to the achievement of an outcome.

**Severe weather** (Conditions météorologiques sévères) – any dangerous meteorological phenomena with the potential to cause damage, serious social disruption, or loss of human life.

**Sexual content** (Contenu sexuel) - is material where the sexual act may not be explicit (detailed) but an intent to cause sexual arousal or titillation is present. It is evident that a mature sexual theme is being displayed or described.

**Shelter in place** (Abris sur place) – emergency response strategy where building occupant are instructed to remain in a safe location within a building during an emergency. In many cases the occupant may be advised to obtain immediate shelter under tables, desks, or other objects that will offer protection against flying glass or debris. Although, shelter in place is a relatively recent strategy used in high-rise buildings in the event of a fire, it has been used commonly in response to other events, such as earthquakes, hazardous material release, bomb threat, etc.

**Shoulder surfing** (Espionnage par-dessus l'épaule) – using direct observation techniques, such as looking over someone`s shoulder, to get information. Shoulder surfing can be used to obtain a wide variety of confidential information. Be aware of your surroundings, when working on or viewing Government information in public spaces.

**Shredding** (Déchiquetage) – a mechanical cutting or grinding method of reducing standard weighs of office paper, electronic media (diskettes, CDs, DVDs), microfilm and microfiche to fragments.

**SIGINT Secure Area** (SSA) or Sensitive Compartmented Information Facility (SCIF) (Zone d'accès réservé SIGINT ou local isolé pour matériel spécial (LIMS) - term for a secure room or datacenter that foils electronic surveillance and suppresses data leakage. An SCIF includes the use of passive methods such as a room enclosed in a tightly sealed metal shield (Faraday cage) and active methods (jamming).

**Signals Intelligence** (SIGINT) (Renseignement électromagnétique) – technical information or intelligence comprise of (individually or in combination) communications intelligence (COMINT), electronic information (ELINT) and foreign instrumentation signals intelligence (FISINT).

**Significant event** (Événement important) - an event, either present or imminent, which has an impact on the Agency and its ability to maintain its critical services.

**Single sealed envelope** (Enveloppe simple scellé) – a single envelope with address, no security markings.

**Situational awareness** (Connaissance de la situation) – having insight into one's environment and circumstances to understand how events and actions will affect business objectives, both now and in the

near future. Having complete, accurate, and current SA is essential in any domain where technological complexity, decision making, and the well-being of the public interact. Because incident management involves predictions and forecasts, SA in the area of IT requires an understanding of the interrelationships between critical services and information, safeguards supporting IT infrastructure and processes, and evolving threats.

**Social Engineering** (Ingénierie sociale) - social engineering is the act of manipulating and winning the trust of users into performing actions or divulging sensitive information. When information is obtained and gathered, it can be used to commit fraud or to provide unauthorized computer system access. Social engineering is the practice of trying to trick or manipulate people into breaking normal security procedures.

**Software integrity** (Intégrité des logiciels) – the process of developing software with minimal vulnerabilities.

**Sole tenant** (Locataire unique) – in buildings occupied solely by one federal department or agency, that department is considered the sole tenant of the building. In such cases, the sole tenant assumes all emergency responsibilities normally associated to the major tenant.

**Sophisticated IT security incident** (Incident complexe de sécurité des TI) – an event, usually initiated by sophisticated threat actors, that is complicated to detect and recover from, causes harm to GC networks and systems, and affects the confidentiality, integrity and availability of information.

**Sophisticated IT security threat** (Menace complexe à la sécurité des TI) - an entity or entities that make use of advanced technologies and tradecraft to penetrate or bypass protective systems and security technologies without being detected.

**Spam Messages** (Pourriels) - are unwanted, unsolicited e-mail messages received from an external address. Most spam messages are advertisements. However, some may be messages with criminal content, such as child pornography and scams.

**Special access** (Accès special) – compartmentalized access to information which is derived from sensitive sources such as SIGINT in accordance with international bilateral agreements, and which requires Canadian citizenship, a Top Secret security clearance, formal indoctrination, and subject interview.

**Special discussion area** (Aire protégée) - an area provided to protect against overhearing which shall be designed and managed according to the security classification or designation of the information being discussed as detailed in the document, "Interim Security Standards: Operating, Directives and Guidelines". Such an area is protected against unauthorized and/or inadvertent speech intercept by audio, visual, optical and/or electronic means.

**Speech secure area** (Aire insonorisée) - any area outside of the Special Discussion Area, but not necessarily immediately adjacent to it, where it is not possible to overhear classified and/or sensitive discussions emanating from the Special Discussion Area. There may be buffer zones between the Special Discussion Area and the Speech Secure Area where discussions emanating, from the Special Discussion Area can be understood.

**Spyware** (Logiciel espion) - spyware is software that is installed on a computer without a user's permission, which intercepts or takes partial control over the user's interaction with the computer. Typically spyware targets the Internet browser (Internet Explorer), causing pop-ups or redirected web pages to appear. Infection can occur through a number of ways, including opening e-mail attachments, clicking links in spam e-mails or visiting certain websites.

**Stalking** (Harcèlement criminel) – section 264 of the Criminal Code refers to "criminal harassment," often described as "stalking", and prohibits a person from certain conduct which harasses or causes another to reasonably fear for their safety – unwanted and repeated stalking following a person (or anyone known to them) from place to place; unwanted and repeated communication directly or indirectly with them; unwanted monitoring of watching their home, office, etc.; or engaging in threatening conduct directed at the other person or any member of their family. Generally it consists of repeated conduct that is carried out over a period of time and which causes you to reasonably fear for your safety or the safety of someone known to you.

**Standard public facsimile network** (Réseau de télécopieurs standards public) - refers to facsimiles attached to a normal phone line.

**Statement of sensitivity** (Énoncé de sensibilité) – provides a detailed description of the system or application from both an operational perspective and a technical perspective. It also provides a list of the valuable or essential assets forming the IT system with an appreciation of the worth of each asset from a financial or business perspective.

**Structural/environmental issues and accidents** (Problèmes et accidents structuraux et environnementaux) – incidents that relate to building structures, or result from weather occurrences and that lead to deficiencies within the building such as floods, gas leaks, water supply issues, etc.

**Subject Matter Expert** (Expert en la matière) – an SME is a contact person within the organization who has an expertise or specialized knowledge in a program, operational or policy area.

**Subscriptions** (Abonnements) - are agreements to receive, participate in or access mailing lists and newsgroups.

**Surge capacity** (Capacité de mobilisation) – The ability to draw upon additional resources to sustain operations and to increase the response, as required.

**Surreptitious attack** (Attaque subreptice) – a secret unauthorized attack to breach or circumvent a defensive system or some of its components in such a manner that the custodians and/or security force cannot readily detect the attack.

**System access administrator** (Administrateur de l'accès au système) – individual who has been assigned security responsibilities to enter and maintain user system access privileges, and activities on Agency information technology (IT) systems.

**System access definitions catalogue** (Catalogue de definitions d'accès aux systèmes) – catalogue that facilitate the administration of systems access rights and which identify the systems access requirements based on the duties performed.

# T

**Table Top Exercise** (Exercice sur table) also referred to as TTX. It is a discussion-based, facilitated group analysis of an emergency situation in an informal stress-free environment.

**Tailgating** (Passage en double) - An individual seeking entry to a restricted area by following a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the door open for the individual. The legitimate person may fail to ask for identification for any number of reasons, or may accept an assertion that the individual has forgotten or lost the appropriate identity token. The individual may also present a fake identity token.

**Target** (Cible) – anything which has or appears to have value for one or more individuals or groups and which, because of its real or perceived value, requires protection.

**Target hardening** (Renforcement des cibles) – the sum of all the inanimate components of a physical security system which protects (or hardens) a given target.

**Technical safeguard** (Mesure de protection technique) - refers to information technology measures used to protect the facility, the equipment, and the support system where personal information is recorded and stored.

**Technical security reviews** (Examens de la sécurité technique) – refers to reviews which are to be completed for all Agency information technology (IT) networks, systems, and applications when being developed or when being modified.

**Telecommunications** (Télécommunications) – transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, visual or other electromagnetic systems. This includes telephone, telegraph, teletype, facsimile, data transmissions, closed circuit television and remote dictation systems.

**Teleconference** (téléconférence) -  the activity of remotely participating to a conference or meeting using the telephone system.

**Telework** (Télétravail) - telework refers to CBSA users who work from an approved remote location (i.e. home or remote sites) or who frequently work, while on travel status, using an approved Secure Remote Access (SRA) laptop.

**Telework place** (Lieu de télétravail) – the location at which an employee and an employer have mutually agreed the employee will work, either at the employee's residence or elsewhere.

**Tempest** (Tempest) - the discipline that deals with the suppression of unintentionally radiated or conducted electromagnetic signals that divulge information.

**Terrorism** (Terrorisme) – unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.

**Theft** (Vol) - a criminal act in which property belonging to another is taken without that person's consent.

**Third party information** (Renseignement de tiers) - as described in Section 20 of the Access to information Act includes trade secrets of a third party, company financial, commercial, scientific or technical information which could affect competitive position or interfere with contractual or other negotiations.

**Threat** (Menace) – potential event or act, deliberate or accidental, that could cause injury to employees, information, assets or services.

**Threat analyses** (Analyses des menaces) – involves steps that are taken to describe the specific nature of an act or condition that could cause injury to Agency personnel, assets or operations. These analyses are descriptive in nature.

**Threat and Risk Assessment** (TRA) (Évaluation de la menace et des risques) – an evaluation of the nature, likelihood and consequences of acts or events that could place employees, information, assets and systems at risk.

**Threat Assessment** (Évaluation de la menace) - an evaluation of the nature, likelihood and consequences of acts or events that could place personnel, Protected or Classified information and assets at risk.

**Threats to the security of Canada** (Menaces envers la sécurité du Canada) - threats to the security of Canada means:

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada, but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

**Timely** (Opportun) – completed or occurring at a favorable or useful time. To be considered timely within the context of risk assessment, the item being looked at must be compared to the operational conditions, threat conditions and environmental conditions and no major changes in relevant information found.

**Top Secret** (Très secret) - applies to information when its compromise could reasonably be expected to cause extremely serious injury to the national interest of Canada. Examples include important and significant negotiations, vital law enforcement and intelligence matters, information classified by CSIS & RCMP regarding strategic plans, criminal or security threats.

**Transitory information** (Renseignements transitoires) - transitory information is information that is required for a limited time to ensure the completion of a routine action or the preparation of a subsequent document. Transitory information includes information in a form used for casual communication, draft versions of documents where comments and additional information are incorporated into subsequent versions, process versions of documents that were not communicated outside the creating office, and duplicate versions of documents used as a reference source only.

**Transmittal** (Transmission) - to send protected and classified information from one person/place to another by a third party. The bearer does not have the need-to-know.

**Transmittal of sensitive information** (Transmission des renseignements sensible) – is the transfer of sensitive information and assets from one person or place to another by someone without a need to know/access to the information/asset (third-party).

**Transmittal outside Canada** (Transmission à l'étranger) – to transmit from Canada, to, from or within GoC facilities (embassies, missions or deployments, department buildings, consulates) in foreign countries.

**Transport of Sensitive Information** (Transporter des renseignements sensible) – is the transfer of sensitive information and assets from one person or place to another by someone with the appropriate screening level and the need to know or access to the information/asset.

**Trojan Horse** (Cheval de Troie) – a Trojan horse is a type of malware that is disguised within a legitimate program while appearing to perform a desirable function. They tend to be invisible to average users, but often include a backdoor allowing unauthorized access to the target`s computer to steal information or harm their host computer systems.

## U

**Unauthorized access** (Accès non autorisé) - access to information and assets by an individual who is not properly security screened and/or does not have a need-to-know.

**Unauthorized access to facility** (Accès non autorisé à l'installation) – any accidental or deliberate access to a CBSA facility by unauthorized persons.

**Unauthorized comments** (Commentaires non autorisés) - only authorized spokespersons can issue statements or make comments about the CBSA's position on a given subject.

**Unauthorized disclosure** (Divulgation non autorisée) – disclosure that is forbidden by law or Government or Agency policies.

**Uncertainty** (Incertitude) - is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

**Update cycle** (Cycle de mise à jour) – relates to the expiry of Reliability Status or security clearances, which are granted for a period of 5 years or 10 years depending on the level. The Agency must update an individual's Reliability Status, Level I (Confidential) and Level II (Secret) security clearances once every ten years. A Reliability Status + and a Level III (Top Secret) security clearance must be updated once every five years

**Useful records** (Documents utiles) - records which can be replaced or reproduced without undue inconvenience or expense to operations.

**User account** (Compte d'utilisateur) - includes all files, folders, e-mail messages or records of accesses to the Internet contained in an account assigned to a user or in a shared drive.

**Uttering threats** (Proférer des menaces) - make abusive, derisive, threatening, insulting, offensive or provocative statements or gestures to or about another person.

## V

**Value** (Valeur) –estimated worth, monetary, cultural, intellectual or other.

**Vandalism of CBSA property** (Vandalisme contre des biens de l'ASFC) – damage to CBSA facility/assets in which no forcible entry occurred (i.e. broken windows, lights, graffiti, etc.).

**Verbal/written abuse - no threat of bodily harm** (Abus verbal et écrit - sans menace de lésion corporelle) – spoken or written words, including printed or electronic messages; pictures, images or gestures that insult, disparage, revile, or malign an employee.

**Video conferencing** (vidéoconférence) - the activity of remotely participating to a conference or meeting through the use of Video camera system (not through the Internet or Intranet).

**Violation** (Infraction) –in terms of any act or condition (intentional or otherwise) which results in a security control being bypassed, defeated or otherwise reduced in its ability to meet management`s expectation with respect to the management of physical security risk .

**Violation of security** (Manquement à la sécurité) - any act or omission that contravenes any provision of the security policies (PGS and CBSA).

**Violent material** (Matériel à caractère violent) - includes material where physically injurious or violent acts or treatment are being depicted.

**Virtual private network** (Réseau privé virtuel) - a restricted-use logical computer network that provides segregation of network traffic often by tunnelling links of the virtual network across the real network. Segregation may be virtual or physical through the use of cryptography, network controls, access controls, or physical separation.

**Visitor** (Visiteur) – an individual whom does not work for the government, but has a legitimate reason for being on the premises and a need to be processed by the control of access system in place.

**Visual sweep** (Examen visuel) – a visual sweep can be conducted in seconds by looking around the immediate area to identify any items that are out of the ordinary or any unidentified threats such as smoke in a hallway.

**Vital Records** (Documents essentiels) – records which are either irreplaceable or whose replacement would involve a critical delay to operations.

**Voice over internet protocol** (Voix sur le protocole Internet) - refers to having a one-on-one conversation over the Internet.

**Vulnerability** (vulnérabilité) — an inadequacy related to security that could increase susceptibility to compromise or injury.

**Vulnerability analyses** (Analyses de la vulnérabilité) - involve steps that are taken to describe the specific nature and elements of an inadequacy related to security that could increase susceptibility to compromise or injury.

**Vulnerability assessment** (Évaluation de vulnérabilité) – the process of identifying and evaluating vulnerabilities, describing all protective measures in place to reduce them, and estimating the likelihood and impact.

## W

**Web 2.0 tools** (Outils Web 2.0) – includes internet-based tools and services that allow for participatory multi-way information sharing, dialogue, and user-generated content. This can include social media and collaborative technologies.

**Web conferencing** (Cyberconférence) - the activity of remotely participating to a conference or meeting through the use of the Internet or Intranet.

**Wide area network** (Réseau étendu) - the network on the outside of a firewall or network that connects to the Internet.

**WiFi** (Wireless Fidelity)- is the trade name for the popular wireless technology used in home networks, mobile phones, video games and more.

**Wireless** (Sans fil) - refers to any technology that communicates via an air interface such as infrared (IR) or radio frequency transmissions instead of closed wiring paths. The term wireless includes all devices, systems and services that have wireless connectivity capabilities.

**Wireless Device** (Appareil sans fil) - refers to any portable device used to access electronic resources, systems, services and networks using wireless technology. Wireless devices include, but are not limited to, cellular phones, pagers, laptops, Personal Digital Assistants (PDAs), satellite communication equipment, two way radios, and peripherals (i.e. mice and keyboards).

**Wireless LAN** (Réseau local sans fil) – A wireless LAN or WLAN is a wireless local area network, which is the linking of two or more computers or devices without using wires.

**Wireless Personal Area Networks** (Réseaux personnels sans fil) - represents wireless personal area network with a very short range. The reach of a WPAN is typically a few meters. WPANs can be used for communication among the personal devices themselves (intrapersonal communication) or for connecting to a higher level network and the internet (an uplink).

**Wireless Priority Service** (WPS) (Service prioritaire sans fil) – WPS is an enhancement to basic mobile service that allows registered essential personnel calls to queue for the next available service channel while minimizing impact on regular consumer access to the same wireless infrastructure.

**Wireless technology** (Technologie sans fil) - technology that permits the transfer of information over a distance without the use of enhanced electrical conductors (wire).

**Wireless Wide Area Networks** (Réseaux étendus sans fil) – WWAN stands for Wireless Wide Area Network, is a form of wireless network. A WWAN differs from a WLAN (wireless LAN) in that it uses cellular network technologies such as WIMAX.

**Witness** (Témoin) - an individual other than the respondent being interviewed for the purpose of obtaining information that includes documentation, relating to an investigation.

**Workplace** (Lieu de travail) – the official location where the employee would originally work.

**Workplace Violence** (Violence en milieu de travail) – an action, conduct, threat or gesture that can reasonably be expected to cause harm, injury or illness to an employee in the workplace.

**Workshop** (Atelier) - a discussion-based exercise that resembles an orientation seminar; however, the participants' interactions is increased and the focus is on achieving or building a product (i.e. a plan, a policy).

**Worldwide interoperability for microwave access** (L'interopérabilité mondiale pour l'accès micro-ondes) - is a telecommunications technology that provides for the wireless transmission of data in a variety of ways, ranging from point-to-point links to full mobile cellular-type access. It is a standards-bases technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.

**Worm** (Ver informatique) – a computer worm is a standalone malware computer program that replicates itself in order to spread to others computers. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm ot the network.

**Wrongdoing** (Acte répréhensible) –

(a) contravention of any Act of Parliament or of the legislature of a province, or of any regulations made under any such Act, other than a contravention of section 19 of this Act (Public Servants Disclosure Protection Act);

(b) misuse of public funds or a public asset;

(c) gross mismanagement in the public sector;

(d) an act or omission that creates a substantial and specific danger to the life, health or safety of persons, or to the environment, other than a danger that is inherent in the performance of the duties or functions of a public servant;

(e) serious breach of a code of conduct established under section 5 or 6; and

(f) knowingly directing or counselling a person to commit a wrongdoing set out in any of paragraphs (a) to (e).

## Z

**Zone** (Zone) – a series of clearly discernible spaces to progressively control access.

2014-12-12/jxs099

# Lexique de la terminologie en sécurité

## A

**Abonnements** (Subscriptions) – ententes conclues pour accéder à des listes d'adresses ou à des groupes de discussion, pour en faire partie ou pour les recevoir.

**Abri sur place** (Shelter in place) – stratégie d'intervention d'urgence dans le cadre de laquelle on demande aux occupants d'un bâtiment de rester dans un lieu sûr, à l'intérieur d'un édifice, lors d'une urgence. Bien souvent, on conseille aux occupants de se mettre à l'abri sous des tables, des bureaux ou d'autres objets qui les protégeront contre les morceaux de verre ou les débris. Si l'abri sur place est une stratégie relativement récente utilisée dans les immeubles de grande hauteur, en cas d'incendie, elle est couramment employée lors d'intervention pour d'autres évènements comme les tremblements de terre, les déversements de matières dangereuses, les alertes à la bombe, etc.

**Abus** (Abuse) – paroles dites ou écrites, y compris les messages imprimés ou électroniques, dessins, images ou gestes qui insultent, dénigrent, vilipendent ou diffament un employé.

**Abus de confiance** (Defalcation) - désigne le détournement de fonds publics et de fonds détenus en fiducie.

**Abus de pouvoir** (Abuse of authority) – fait de se prévaloir d'une situation d'autorité de façon abusive. L'abus de pouvoir peut prendre de multiples formes (p. ex. profiter d'une personne ou simplement la manipuler en ayant le pouvoir de la sanctionner si elle n'obéit pas). Fait d'exercer son pouvoir ou son influence de façon indue ou inappropriée sur un subordonné au moyen de méthodes sournoises ou manipulatrices.

**Abus physique** (Physical abuse) – fait d'utiliser de façon délibérée la force contre une personne sans son consentement. Comprend les voies de fait. Peut causer des douleurs physiques ou des blessures à long terme.

**Abus verbale et écrit** – sans menace de lésion corporelle (Verbal/written abuse – no threat of bodily harm) – paroles dites ou écrites, y compris les messages imprimés ou électroniques, dessins, images ou gestes qui insultent, dénigrent, vilipendent ou diffament un employé

**Accès (TI)** (Access IT) - entrée en communication avec une ressource électronique fournie par l'ASFC à des personnes autorisées ou utilisation de cette ressource. L'accès à de telles ressources peut se faire dans les locaux du gouvernement ou ailleurs. L'accès permet le télétravail et l'utilisation à distance. Il s'entend aussi de l'utilisation, par des personnes autorisées, des ressources électroniques fournies par

l'ASFC à des fins personnelles limitées, en dehors des heures de travail, tel qu'il est prévu par la politique.

**Accès à Internet anonyme** (Anonymous internet access) – accès à Internet qui ne permettra pas d'identifier l'utilisateur d'un organisme en tant que tel.

**Accès non autorisé** (Unauthorized access) – accès à des renseignements et à des biens par un particulier qui n'a pas fait l'objet d'une enquête de sécurité du personnel ou ne satisfait pas aux critères du besoin de connaître, ou les deux.

**Accès non autorisé à l'installation** (Unauthorized access to facility) – tout accès accidentel ou délibéré par des personnes non autorisées à une installation de l'ASFC.

**Accès privilégié** (Privileged access) − Autorisation ou ensemble d'autorisations qui permet aux utilisateurs de contourner les mesures de contrôle d'accès logiques pour exécuter des fonctions qui sont habituellement interdites aux utilisateurs ordinaires (non privilégiés).

**Accès spécial** (Special Access) – accès compartimenté à de l'information issue de sources sensibles telles que le renseignement électromagnétique (SIGINT), conformément aux accords bilatéraux internationaux, et qui exige, pour le titulaire de cet accès, la citoyenneté canadienne, une cote de sécurité Très secret ainsi que la réalisation d'une initiation officielle et d'une entrevue en personne.

**Accréditation** (Accredidation) – autorisation officielle par la direction d'exploiter un système des TI et acceptation par la direction du risque résiduel s'y rattachant. L'accréditation dépend des résultats de la certification ainsi que d'autres considérations de nature administrative.

**Accusé de réception** (Hand receipt) - document comptable servant à enregistrer la remise d'un matériel COMSEC à un utilisateur autorisé et l'acceptation de la responsabilité par ce dernier du matériel remis.

**Acte répréhensible** (Wrongdoing)

a) contravention d'une loi fédérale ou provinciale ou d'un règlement pris sous leur régime, à l'exception de la contravention de l'article 19 de la présente loi (Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles);

b) usage abusif des fonds ou des biens publics;

c) cas graves de mauvaise gestion dans le secteur public;

d) fait de causer — par action ou omission — un risque grave et précis pour la vie, la santé ou la sécurité humaine ou pour l'environnement, à l'exception du risque inhérent à l'exercice des attributions d'un fonctionnaire;

e) contravention grave d'un code de conduite établi en vertu des articles 5 ou 6;

f) fait de sciemment ordonner ou conseiller à une personne de commettre l'un des actes répréhensibles visés aux alinéas a) à e).

**Activité personnelle** (Private business) – activité entreprise en dehors du cadre professionnel à des fins de gain ou de profit personnel. Comprend la vente ou l'achat de biens ou de services. L'activité politique entre également dans cette catégorie.

**Administrateur de l'accès au système** (System Access Administrator) – personne qui s'est vu confier les responsabilités en matière de sécurité pour inscrire et mettre à jour les privilèges d'accès aux systèmes des utilisateurs et les activités liées aux systèmes des technologies de l'information (TI) de l'Agence.

**Administrateur général** (Deputy Head) - le terme « administrateur général » tel qu'il est défini à l'article 11 de la Loi sur la gestion des finances publiques, et, dans le cas des Forces canadiennes, le chef de l'État-major de la Défense.

**Administration centralisée des comptes d'utilisateurs** (Consolidated User Administration) – Centralisation des comptes d'utilisateurs et de l'administration de la sécurité pour accéder aux applications de l'ARC/de l'ASFC.

**Administration de contenu** (Content administration) – peut inclure, entre autres, l'activation des messages d'absence du bureau ou l'extraction des documents internes.

**Administration de la sécurité et coordination du programme** (Security administration and program coordination) - établissement de documents sur les politiques, normes, lignes directrices, procédures et plans de référence relatifs aux exigences de sécurité internes et établissement des mécanismes appropriés associés aux ententes concernant des biens ou des risques partagés entre divers organismes.

**Agent de sécurité du ministère** (Departmental security officer) – responsable d'établir et de diriger le programme de sécurité de l'Agence.

**Agent de surveillance du renseignement sur les communications (COMCO)** (Communications intelligence control officer) – est responsable de la gestion et de la supervision de l'information classifiée et sensible d'intérêt pour le renseignement national et définie et désignée comme documents spéciaux. Les documents spéciaux représentent toute information ou tout document exigeant une surveillance particulière pour en garantir la manipulation restreinte, avec les systèmes compartimentés du renseignement étranger. Les documents spéciaux comprennent notamment le renseignement d'origine électromagnétique (SIGINT).

**Agent désigné** (Designated officer) - agent désigné par le président en vertu de l'article 163.4 de la Loi sur les douanes. Selon le paragraphe 163.5, l'agent des douanes désigné a les pouvoirs et obligations que les articles 253 et 254 et 495 à 497 du Code criminel confèrent à un agent de la paix.

**Aire insonorisée** (Speech secure area) – endroit à l'extérieur de l'aire protégée sans nécessairement y être adjacent, d'où il est impossible d'entendre des discussions de niveau classifié ou confidentiel émanant de l'aire protégée. Il peut y avoir des zones tampons entre l'aire protégée et l'aire insonorisée d'où il est possible d'entendre les discussions qui proviennent de l'aire protégée.

**Aire protégée** (Special discussion area) – salle à l'épreuve de l'écoute accidentelle; elle doit être conçue et aménagée aux termes des normes de sécurité, où l'on doit définir le niveau de classification des informations pouvant y être discutées selon les directives du document intitulé « Normes provisoires de sécurité - Directives et lignes directrices d'utilisation ». Cet endroit est conçu de façon à éviter les interceptions délibérées ou accidentelles de conversations au moyen de techniques acoustiques, visuelles, optiques ou électroniques.

**Alerte** (Alert) – indication « instantanée » qu'un système d'information et un réseau peuvent faire l'objet d'une attaque ou être compromis en raison d'un accident, d'une défaillance ou d'une erreur humaine.

**Alerte à la bombe** (Bomb threat) – menace, généralement verbale ou écrite, de faire exploser un engin explosif ou un dispositif incendiaire afin de causer des blessures, des dommages aux biens ou de provoquer la mort, qu'un tel engin existe ou non.

**Analyse des répercussions sur les applications** (Application impact analysis) – processus complémentaire de l'analyse des répercussions sur les opérations (ARA) et moyen utilisé pour mettre en correspondance les applications, systèmes, et matériel de TI et les fonctions opérationnelles.

**Analyse des répercussions sur les opérations** (Business impact analysis) – une analyse des répercussions sur les opérations est un outil afin d'évaluer l'impact des perturbations sur le département et d'identifier et de prioriser les services essentiels et les biens associés.

**Analyses de la vulnérabilité** (Vulnerability analyses) – comprend les étapes prises pour décrire la nature et les composantes précises d'une insuffisance liée à la sécurité qui pourrait accroître la susceptibilité à la compromission ou au préjudice.

**Analyses des menaces** (Threat analyses) – Les analyses des menaces comprennent des mesures qui sont prises pour décrire la nature précise d'un geste ou d'une condition qui risque de porter préjudice aux employés, à des biens ou aux activités de l'Agence. Ces analyses sont descriptives de nature.

**Antivirus** (Antivirus) - Un antivirus est un logiciel de sécurité spécialisé qui détecte les formes connues de logiciels malveillants. Il ne se limite pas qu'aux virus, mais peut s'avérer inefficace contre certaines formes de malicieux, comme les programmes malveillants furtifs

**Appareil sans fil** (Wireless Device) – s'entend de tout appareil portable utilisé pour accéder aux ressources, systèmes, services et réseaux électroniques au moyen de la technologie sans fil. Les appareils sans fil comprennent, entre autres, les téléphones cellulaires, les téléavertisseurs, les portables, les assistants numériques (PDA), le matériel de communication satellitaire, les émetteurs-récepteurs et les périphériques, notamment les souris et claviers.

**Articles cryptographiques contrôlés** (Controlled cryptographic items) – dispositifs de chiffrement des liens approuvés par le Centre de la sécurité des télécommunications Canada (CSTC) et qui sont utilisés

pour protéger la confidentialité et l'intégrité des renseignements Protégé C et classifiés lorsqu'ils sont transmis à l'aide de moyens électroniques. Deux CCI compatibles sont nécessaires pour établir une connexion sécuritaire.

**Association criminelle** (Criminal association) - association de personnes ou de groupes que l'on soupçonne d'être liés à des activités criminelles. Cette association restreinte couvre toute relation à caractère social, sexuel, financier ou commercial avec une source d'information, un criminel notoire ou présumé ou une personne qui fait l'objet d'un renvoi du Canada.

**Association de données à l'infrarouge** (Infrared Data Association) – une norme régissant la communication sur de courtes distances entre les dispositifs, comme les ordinateurs, les assistants numériques (PDA) et les téléphones cellulaires, au moyen de signaux infrarouges.

**Assurance** (Assurance) – degré de certitude concernant la véracité d'un énoncé ou d'un fait.

**Assurance de justificatif d'identité** (Assurance of credential) – caractère exécutoire du justificatif d'identité d'une personne (sans égard à l'identité de cette dernière).

**Assurance de l'identité** (Assurance of identity) – a trait à l'affirmation que la personne est bien celle qu'elle prétend être. Ces deux assurances (l'assurance de justificatif d'identité et l'assurance de l'identité) sont requises pour assurer l'efficacité de la méthode d'authentification.

**Assurance de l'identité** (Identity assurance) − Un niveau de certitude qu'une personne, un organisme ou un appareil est bien celui qu'il prétend être.

**Assurance des justificatifs** (Credential assurance) − S'entend de l'assurance qu'une personne, une organisation ou un appareil a conservé le contrôle de ce qui lui a été confié (p. ex. clé, jeton, document, identificateur) et que le justificatif n'a pas été compromis (p. ex. falsifié, modifié).

**Atelier** (Workshop) – exercice axé sur la discussion qui ressemble à un séminaire d'orientation, mais comporte plus d'interactions entre les participants et où on vise à réaliser ou à élaborer un produit (p. ex. un plan ou une politique).

**Attaque** (Attack) – Toute action pour mettre à exécution la menace.

**Attaque** (TI) (Attack IT) – tentatives visant à exploiter la vulnérabilité d'un système de TI ou à détruire, à exposer, à altérer ou à rendre inopérants un système d'information ou les données contenues dans un système d'information, que l'on désigne également sous le terme de « cyberattaque ».

**Attaque subreptice** (Surreptitious attack) – attaque secrète et non autorisée visant à percer ou à contourner un système de protection ou certaines de ses composantes de manière à ce que les gardiens ou la force d'intervention ne puissent la détecter facilement.

**Atteinte à la sécurité** (Security Violation) – tout acte ou toute omission qui fait en sorte qu'une personne ou une entité tente de contourner, d'éviter ou d'éliminer un contrôle de sécurité, ou de

réduire son efficacité. Il importe de faire ressortir qu'il existe diverses formes ou divers niveaux de gravité d'atteintes à la sécurité

**Atteinte à la vie privée** (Privacy breach) – création, collecte, utilisation, divulgation, conservation ou disposition inappropriée ou non autorisée de renseignements personnels.

**Atténuation** (Mitigation) – mesures soutenues prises pour éliminer ou réduire les risques et les répercussions découlant des dangers bien avant qu'un incident ou un sinistre survienne. Les activités d'atténuation pourraient faire partie des moyens de prévention.

**Atténuation du risque** (Risk mitigation) – processus intégré à l'environnement des contrôles, notamment aux politiques, aux cadres et aux responsabilités, visant à atténuer le niveau de risque résiduel (risque restant réduit à un niveau acceptable).

**Attestation de sécurité d'installation** (Facility security clearance) - an administrative determination that an organization is eligible, from a security viewpoint, for access to classified and protected information or assets of the same or lower classification level as the clearance being granted.

**Attestation de sécurité du personnel** (Personnel security clearance) - processus permettant de s'assurer que les personnes qui ont accès aux renseignements, aux biens et aux services du gouvernement sont honnêtes, dignes de confiance, fiables et loyales à l'égard du Canada.

**Auteur** (Author) – personne responsable de la création ou de la collecte de renseignements.

Authentification (Authentication) – identification positive, assortie d'un degré de certitude suffisant pour autoriser certains droits ou privilèges à la personne ou à l'élément reconnu formellement. En termes simples, il s'agit de vérifier l'identité déclarée d'une personne, d'une station ou d'un émetteur.

**Autorisation** (Authorization) – octroi, à un utilisateur, à un programme ou à un processus, du droit d'accès à un système de TI par le propriétaire ou le contrôleur d'un système de technologie de l'information.

**Autorité** (Authority) – L'organisation à qui l'équipe de la direction a conféré le pouvoir d'élaborer, d'approuver ou d'interrompre l'exécution d'une fonction de sécurité de la TI ou de travaux connexes.

**Autorité COMSEC** (COMSEC authority) – personne responsable de la sécurité et de la comptabilisation de l'information et des biens COMSEC en élaborant la politique et les normes COMSEC de l'Agence et en fournissant des conseils à l'égard des exigences COMSEC.

**Autorité COMSEC du ministère** (Departmental COMSEC authority) - personne désignée par l'agent de sécurité du ministère et responsable devant celui-ci d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller un programme COMSEC du ministère qui soit conforme à la Politique sur la sécurité du gouvernement et aux normes qui s'y rattachent.

**Autorité de certification** (Certification authority) – personne ou entité qui délivre des certificats de signature numérique et qui est inscrite en cette qualité sur le site Web du Secrétariat du Conseil du Trésor.

**Autorité de contrôle** (Controlling authority) - responsable désigné pour gérer l'utilisation et le contrôle opérationnels des clés attribuées à un réseau cryptographique.

**Autorité et orientation fonctionnelles** (Functional authority and direction) - orientation et rendement d'un programme particulier (p. ex. conception, mise en œuvre et mise à jour d'un programme et de politiques, allocation des ressources, offre de conseils et d'orientation pour le programme, suivi et établissement de rapports sur le rendement du programme, etc.).

**Autorité hiérarchique** (Line authority) – organisation supérieure à une personne ou à une partie de l'organisation qui détermine l'ordre de priorité des tâches, attribue les ressources, surveille l'exécution du travail tout en étant responsable de la prestation des services, à divers degrés. Tandis qu'une personne rend directement des comptes à son supérieur hiérarchique, le caractère approprié du travail est souvent déterminé en fonction des exigences des autorités fonctionnelles au sein d'une organisation.

**Autorité responsable de l'immeuble** (ARI) (Responsible Building Authority) - Où l'ASFC est le seul locataire ou l'installation est partagée avec le secteur privé, l'ARI est défini comme le plus haut fonctionnaire de l'ASFC. Où l'ASFC est situé dans un environnement multi-locataire, le plus haut fonctionnaire des principaux "gouvernement" locataire est considéré comme le ARI.

**Autres renseignements** (Other information) – Le terme utilisé pour décrire la grande quantité de renseignements du gouvernement qui ne sont pas des renseignements à classifier dans l'intérêt national ni à protéger comme autres renseignements de nature délicate.

**Avis de confidentialité** (Privacy notice) – Avis présenté à un individu afin de communiquer les fins de la collecte de renseignements personnels, et l'autorité de l'institution fédérale pour procéder à la collecte, à l'utilisation et à la divulgation des renseignements pour un programme ou une activité donnée. L'avis informe également l'individu de ses droits d'accès et de correction de ses renseignements personnels, ainsi que des conséquences du refus de fournir les renseignements demandés

# B

**Bavardoirs** (Chat rooms) aussi connus sous le nom de Forum de discussions – forums électroniques qui permettent aux participants d'avoir une discussion en ligne en temps réel, généralement par l'échange de messages textes.

**Besoin de connaître** (Need to Know) – besoin éprouvé par une personne d'accéder à des renseignements et de les connaître pour accomplir les tâches qui lui incombent. L'accès aux installations, aux systèmes et à l'information est limité aux seuls utilisateurs qui ont « besoin de connaître ». Cela signifie que l'accès est accordé uniquement aux utilisateurs ayant la cote de sécurité

appropriée, et que les utilisateurs ont seulement accès à l'information et aux systèmes dont ils ont besoin pour pouvoir s'acquitter de leurs fonctions.

**Biclé** (Key pair) – paire de clés détenue par ou pour une personne comportant une clé privée et une clé publique qui sont mathématiquement liées tout en étant différentes l'une de l'autre.

**Bien essentiel** (Critical asset) – actif soutenant la prestation d'un service indispensable dont la compromission porterait un préjudice élevé à la santé, à la sécurité ou au bien-être économique des Canadiens, ou encore au fonctionnement efficace du gouvernement du Canada.

**Biens contrôlés** (Controlled assets) – Les biens qui ont été évalués à titre de biens nécessitant des contrôles de sécurité internes spécialisés et qui sont intégrés aux opérations courantes tout au long de leur cycle de vie à partir du moment de leur acquisition, pendant leur transit, leur réparation, leur entretien, leur retour et leur destruction. Les biens contrôlés comprennent, entre autres, les insignes, les cartes d'identité, les fiches d'autorité, les cartes de désignation, les armes à feu et les munitions ainsi que les timbres de l'ASFC.

**Biens** (Asset) – éléments d'actifs corporels ou incorporels du Gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale.

**Biens classifiés** (Classified assets) – biens dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national.

**Biens de nature délicate** (Sensitive Assets) – biens qui nécessitent une protection supplémentaire en raison de leur valeur ou du préjudice que causerait leur destruction, retrait, modification, interruption, perte, divulgation, mauvaise utilisation ou accès non autorisé.

**Biens protégés** (Protected assets) – biens ou information susceptibles d'être visés par une exclusion ou une exception en vertu de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels, car la divulgation ou l'accès sans autorisation risquerait vraisemblablement de porter préjudice à un particulier ou à une organisation.

**Biens publics** (Public property) – désigne tous les biens (y compris les données), autres que les fonds publics, qui appartiennent à sa Majesté du chef du Canada.

**Blasphème** (Profanity) – comprend, notamment, les documents utilisant un langage vulgaire (offensant), le langage vulgaire employé dans les textes écrits, l'usage verbal de termes offensants dans un fichier sonore ou une vidéo ou même les sous-titres des images.

**Bluetooth** (Bluetooth) – technologie sans fil de communications radio de faible portée facilitant la transmission des données sur de courtes distances à partir d'appareils fixes et mobiles visant à créer des réseaux personnels sans fil (PANs). Technologie plus souvent utilisée pour connecter les appareils en évitant les inconvénients des câbles et des prises murales.

**Bureau national des incidents COMSEC** (National COMSEC incidents office) - entité du Centre de la sécurité des télécommunications Canada chargée de gérer les incidents COMSEC, par l'enregistrement, l'enquête, l'évaluation et la fermeture des dossiers, et d'assurer la liaison et la coordination directes avec les autres bureaux d'incidents COMSEC nationaux et internationaux.

**But de l'exercice** (Exercise aim) – souligne la finalité de l'exercice (p. ex. évaluer si l'ASFC est bien préparée pour faire face à l'arrivée d'un navire transportant des migrants).

## C

**Cadre supérieur** (Executive) – Un employé nommé à un poste du groupe de la direction (d'EX-01 à EX-05), c'est-à-dire à un poste de directeur, de directeur général, de sous-ministre adjoint ou à un poste équivalent.

**Capacité de mobilisation** (Surge capacity) – capacité de miser sur des ressources additionnelles en vue de soutenir les opérations et de consolider le processus d'intervention, au besoin.

**Carte d'identité** (Identification card) – document fourni par un ministère ou une organisation qui permet d'identifier le détenteur. La carte d'identité ne doit pas être confondue avec l'insigne d'accès, car ils n'ont pas la même finalité ni le même aspect physique.

**Carte de désignation** (Designation card) – le président peut nommer tout agent pour appliquer la partie VI.1 de la Loi sur les douanes (contrôle d'application en matière d'infractions criminelles à d'autres lois, en vertu de cette Loi) et lui délivrer un certificat de désignation.

**Catalogue de définitions d'accès aux systèmes** – (System access definitions catalogue) catalogue qui facilite l'administration des droits d'accès aux systèmes et permet d'identifier les exigences d'accès aux systèmes en fonction des tâches à accomplir.

**Catastrophe** (Disaster) – événement catastrophique soudain et imprévu causant des dommages ou des pertes inacceptables; compromet la capacité de l'organisation à assurer les fonctions, processus ou services indispensables pendant une période de temps inacceptable ou oblige la direction à suspendre ses activités de fonctionnement habituelles et à exécuter son plan de continuité des activités ou son plan de de reprise des TI suite à une catastrophe.

**Catégories de renseignements personnels** (Classes of personal information) – renseignements personnels dont on ne prévoit pas faire usage pour des fins administratives ou que l'on ne peut pas retrouver par référence au nom d'un individu ou à une indication identificatrice propre à cet individu (p. ex. opinions non sollicitées et correspondance générale).

**Catégorisation** (Categorization) – niveau de classification de l'information ou des biens qui fournit une indication quant au degré de risques de préjudice que leur divulgation présenterait pour des intérêts non reliés à l'intérêt national (protégés) ou nationaux (classifiés).

**Centre de repli** (Alternate site) – lieu auxiliaire maintenu à divers états de préparation et utilisé pour traiter des données ou assurer la prestation de services indispensables en cas de perturbation. Remarque : Il y a quatre sortes de centres de repli : les centres de relève immédiate, les centres de relève, les salles blanches et les centres miroir.

**Centre des opérations d'urgence** (Emergency Operation Centre) - Installation désignée par un organisme ou une administration pour coordonner son intervention et l'ensemble de ses activités de soutien en situation d'urgence.

**Certificat de clé publique** (Public key certificate) – information d'une entité apparaissant sur la clé publique signée par une autorité de certification pertinente et qui est par conséquent infalsifiable.

**Certificat de signature numérique** (Digital signature certificate) – à l'égard d'une personne, document électronique qui, à la fois : a) identifie l'autorité de certification qui l'a délivré et est signé numériquement par celle-ci; b) identifie la personne ou peut servir à l'identifier; c) renferme la clé publique de cette personne.

**Certification** (Certification) – évaluation complète des dispositifs de sécurité techniques et non techniques d'un système de TI et d'autres mesures de sauvegarde connexes, effectuée à l'appui de l'accréditation, pour déterminer le degré selon lequel un modèle de conception et de mise en œuvre précis satisfait à un ensemble donné d'exigences de sécurité.

**Chaîne de lettres** – (Chain letters) - messages par courriel ayant une seule finalité, l'envoi à d'autres personnes; promettent faussement de la chance, de l'argent ou d'exaucer un vœu si vous réacheminez le message.

**Cheval de Troie** (Trojan Horse) - un cheval de Troie est un type de logiciel malveillant déguisé en un logiciel légitime et qui semble accomplir la fonction désirée. Habituellement invisible pour l'utilisateur moyen, il permet souvent d'accéder sans autorisation à l'ordinateur visé afin de voler de l'information ou d'endommager les systèmes informatiques hôtes.

**Chiffrement** (Encryption) – transformation d'un message vocal ou de données en format inintelligible par l'utilisation d'un processus cryptographique réversible faisant appel à du matériel ou à un logiciel informatique. Pour lire un fichier chiffré, vous devez avoir accès à une clé secrète ou à un mot de passe qui vous permet de déchiffrer le fichier. Les données non chiffrées sont appelées texte en clair alors que les données chiffrées sont appelées texte chiffré. Il y a deux types de chiffrement, à savoir le chiffrement asymétrique (nommé également chiffrement à clé publique) et le chiffrement symétrique.

**Cible** (Target) – tout élément qui a ou semble avoir de la valeur pour une personne ou un groupe, ou plusieurs, et qui, en raison de sa valeur réelle ou perçue, requiert une protection.

**Clé** (Key) – dispositif utilisé pour ouvrir ou fermer les portes, les armoires et les contenants; incluant les clés en métal et les cartes d'accès électroniques.

**Clé de chiffrement** (Encryption key) – phrase passe ou algorithme nécessaire pour coder un texte en texte chiffré.

**Clé de contact cryptographique** (Crypto-ignition key) - dispositif ou clé électronique utilisé pour déverrouiller le mode sécurisé d'un équipement cryptographique.

**Clé électronique** (Electronic key) - clé stockée sur un support magnétique, sur un support optique ou dans une mémoire électronique, transférée par circuits électroniques ou chargée dans un équipement COMSEC.

**Clé Noire** (Black key) – clé chiffrée (p. ex. matériel de chiffrement classifié qui a été chiffré à l'aide d'une cryptographie approuvée par le Centre de la sécurité des télécommunications Canada).

**Clé privée** (Private key) – suite de données qui est utilisée dans un système de chiffrement à clé publique pour chiffrer des données contenues dans un document électronique; est propre à la personne qui est identifiée dans le certificat de signature numérique ou au moyen de celui-ci, et correspond exclusivement à la clé publique reprise dans le certificat.

**Clé publique** (Public key) – suite de données contenue dans un certificat de signature numérique qui, à la fois : a) est utilisée dans un système de chiffrement à clé publique pour déchiffrer des données contenues dans un document électronique qui ont été chiffrées au moyen de la clé privée d'une biclé; b) correspond exclusivement à cette clé privée.

**Client** (Client) - bénéficiaire auquel est destiné un extrant de service. Les clients externes sont généralement des particuliers (citoyens canadiens, résidents permanents, etc.) et des entreprises (des secteurs public et privé). Les clients internes sont généralement des agents contractuels et des employés du gouvernement du Canada.

**Cloisonnement** (Compartmentalization) – le fait de diviser une installation/surface utile en plus petites zones et de contrôler l'accès à chacune. Les personnes n'obtiennent des privilèges d'accès que pour les zones auxquelles elles doivent accéder pour pouvoir s'acquitter de leurs fonctions

**Code canadien du travail** (Canada Labour Code) – Partie II du Code canadien du travail sur la santé et sécurité au travail fournit des conseils au gouvernement fédéral pour prévenir les accidents et les blessures. Cela comprend des mesures pour protéger les employés (par exemple, la prévention de la violence dans le lieu de travail).

**Code malveillant** (Malicious Code) – Élément conçu pour créer des virus, des chevaux de Troie ou des vers informatiques et, de façon générale, tout programme ou code conçu pour créer des problèmes informatiques plutôt que pour régler les problèmes existants.

**Coffre de sécurité** (Security container) – espace de rangement de biens classifiés entièrement fermé et conçu pour résister à la force et à des attaques subreptices; p. ex., coffre-fort, armoire de sécurité, coffret de sécurité, chambre forte, chambre forte démontable ou pièce sécuritaire.

**Collecte indirecte** (Indirect collection) - collecte de renseignements personnels auprès d'une source autre que la personne visée.

**Commandant du lieu de l'incident** (Incident commander) – La personne responsable de la gestion de toutes les opérations à l'endroit où l'incident s'est produit.

**Commentaires non autorisés** (Unauthorized comments) – seuls les porte-paroles autorisés peuvent faire des déclarations ou formuler des commentaires au sujet de la position de l'ASFC sur un sujet donné.

**Composant** (Component) – éléments constitutifs d'un système.

**Compromission** (Compromise) – l'accès, la divulgation, la destruction, la suppression, la modification, l'utilisation ou l'interruption non autorisés de biens ou de renseignements.

**Compromission des mesures de protection** (Compromise of security controls) –compromission des mesures de protection utilisées pour protéger les biens, l'information et les employés, ce qui entraîne une augmentation des menaces et des vulnérabilités (mots de passe, clés de chiffrement, serrures, etc.).

**Compromission et interruption** (Compromission/interruption) – abandon, perturbation ou suspension à l'improviste de services, de programmes ou d'activités, ce qui cause une perte de productivité ou une interruption de service.

**Compte COMSEC** (COMSEC account) – entité administrative à laquelle a été attribué un identificateur du Système de gestion électronique des clés (p. ex. un numéro de compte COMSEC) et servant à la comptabilité, à la garde et au contrôle du matériel COMSEC qui lui a été confié.

**Compte d'utilisateur** (User account) – le compte d'utilisateur comprend tous les dossiers, fichiers, messages courriels ou documents d'accès à Internet qui font partie d'un compte assigné à un utilisateur ou qui se trouvent sur un disque partagé.

**Compte rendu post action** (After action report) – également appelé CRPA. Document qui renferme des observations, les forces, les faiblesses, une analyse et les recommandations d'amélioration mises de l'avant lors de l'évaluation de la planification d'un exercice, de son déroulement et du soutien connexe.

**Compte rendu post évènement** (After event report) – également appelé CRPE. Document qui fournit, à la suite d'un évènement, une rétroaction aux hauts fonctionnaires, à la direction et au personnel opérationnel.

**Compte rendu post incident** (After incident report) – également appelé CRPI. Document qui fournit, à la suite d'un incident, une rétroaction aux hauts fonctionnaires, à la direction et au personnel opérationnel.

**COMSEC – Sécurité des communications** – (Communications Security) - L'application de mesures de sécurité cryptographique, de sécurité des transmissions et des émissions et de sécurité matérielle ainsi

que de pratiques et de mécanismes de contrôle opérationnels pour empêcher tout accès non autorisé à l'information issue de télécommunications et pour garantir l'authenticité de ces télécommunications.

**Conditions météorologiques sévères** (Severe weather) – tout phénomène météorologique dangereux susceptible de causer des dommages, une grave perturbation sociale ou des pertes humaines.

**Conduite déshonorante** (Discreditable conduct) – conduite pendant et après les heures de travail susceptible de ternir la réputation de l'employé, celle de l'Agence ou les deux.

**Confidentialité** (Confidentiality) – qualité conférée à des renseignements pour signifier qu'ils ne peuvent être divulgués qu'à des personnes autorisées, afin de prévenir tout préjudice à l'intérêt national ou à d'autres intérêts, comme l'indiquent des dispositions précises de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels.

**Confidentiel** (Confidential) - s'applique aux renseignements pour lesquels il est raisonnable de croire que leur compromission risquerait de porter préjudice à l'intérêt national du Canada. Les exemples comprennent les renseignements associés aux négociations avec les provinces, aux stratégies, tactiques et aux rapports économiques et politiques sur les autres nations, qui ne sont pas accessibles au public au Canada. Parmi les documents de niveau confidentiel, citons les documents stratégiques sur les taux d'intérêt et la politique en matière d'inflation, ou les comptes rendus de discussions des comités interministériels fédéraux.

**Conflit d'intérêts** (Conflict of interest) – s'entend d'une situation où un employé a des intérêts personnels susceptibles d'influencer le rendement de ses fonctions et responsabilités officielles ou utilise sa position à des fins de gain personnel. Un conflit d'intérêts réel existe dans le moment présent, un conflit d'intérêts apparent est une situation qui pourrait être perçue comme telle par une personne raisonnable, que ce soit ou non le cas, tandis qu'un conflit d'intérêts potentiel est une situation qui pourrait raisonnablement survenir, à l'avenir.

**Conformité** (Compliance) – capacité d'assurer de manière raisonnable le respect des politiques, des plans, des procédures, des lois, des règlements et des contrats de l'organisation, et la conformité à ceux-ci.

**Connaissance de la situation** (Situational awareness) – être au fait de son environnement et de ce qui se passe pour comprendre comment les événements et les mesures influera sur les objectifs opérationnels, maintenant et à l'avenir. Les prédictions et les prévisions font partie de la gestion des incidents et il est donc nécessaire, en contexte de CS de la TI, de comprendre l'interrelation entre les services indispensables et l'information, les mesures de protection soutenant l'infrastructure de TI, les processus et l'évaluation des menaces.

**Conseiller en sécurité** (Conseiller en sécurité) – membre du bureau local de sécurité qui fournit des conseils et du soutien en matière de sécurité au chapitre des activités d'intervention d'urgence; en tant que membre de l'organisation de secours de l'immeuble, le conseiller en sécurité ne doit pas avoir de responsabilités précises.

**Constatations** (Findings) – observations factuelles d'une personne compétente sur les éléments trouvés et qui sont justifiables par l'observation, la documentation ou la corroboration.

**Construction d'installation** (Constructing facilities) – installations construites par le gouvernement ou par des propriétaires du secteur privé à la demande du gouvernement.

**Contenant de sécurité approuvé** (Approved security container) – types particuliers de contenants répondant aux normes établies à cette fin.

**Contenu sexuel** (Sexual content) – matériel où l'acte sexuel n'est pas forcément explicite (détaillé) mais dont l'intention est de causer l'excitation sexuelle ou la titillation. Un tel contenu affiche ou décrit clairement un thème de sexualité adulte.

**Continu** (Continued) – peut être interrompu mais doit être rétabli dans un délai acceptable.

**Contrôle continu** (Continuous monitoring) – vérification des biens sous surveillance par le personnel en charge des biens, des gardiens ou par l'entremise de moyens électroniques, assez régulièrement pour détecter les tentatives d'accès non autorisé.

**Contrôle d'accès** (Access control) – le contrôle d'accès permet d'assurer l'accès autorisé aux biens à l'intérieur d'une installation ou de zones d'accès restreint en effectuant une enquête de sécurité sur les employés et en utilisant des dispositifs de contrôle d'accès (p. ex. clés, cartes d'identité, cartes d'accès, gardes de sécurité, etc.).

**Contrôle d'accès (TI)** (Access control IT) – fournit un moyen de faire appliquer la politique d'autorisation. Les mécanismes de contrôle d'accès permettent de faire appliquer les politiques d'autorisation et de définir qui peut accéder aux ressources et dans quelles conditions.

**Contrôle de l'accès** (Control of access) – assurer l'accès autorisé aux biens à l'intérieur d'une installation ou de zones d'accès restreint, en effectuant le triage des employés, des visiteurs et du matériel aux points d'entrée par les membres du personnel, des gardiens ou de façon informatisée et, lorsque requis, en surveillant leur déplacement à l'intérieur de l'installation ou des zones d'accès restreint en les accompagnant.

**Contrôle de sécurité** (Security control) – mesure administrative, opérationnelle, technique, physique ou juridique visant à gérer les risques pour la sécurité. Cette expression est synonyme de protection.

**Contrôle du contenu** (Content monitoring) – peut inclure, notamment, la visualisation du contenu et l'analyse du volume des dossiers, des messages de courriel ou des registres afin de déterminer s'il y a eu mauvaise utilisation.

**Contrôleur/animateur** (Controllers/facilitators) - agent de confiance qui gère la conduite des exercices. Il dirige et surveille le rythme et l'intensité de l'exercice pour assurer la sécurité et l'atteinte des objectifs.

**Coordonnateur de la Gestion de risques des utilisateurs privilégiés** (Privileged user risk management) – Toutes les autorisations privilégiées d'accès aux systèmes doivent être accordées et retirées par le programme de la gestion des risques des utilisateurs privilégiés (GRUP) et elles sont valides pour une période déterminée.

**Correspondance mal acheminée de nature sensible** (Sensitive misdirected correspondence) – les incidents de ce type comprennent ce qui pourrait attirer l'attention des médias, les divulgations très médiatisées ou les refus de renvoyer la correspondance.

**Corruption de données** – (Data corruption) - compromission de l'intégrité de données.

**Cote de fiabilité** (Reliability status) – une cote de fiabilité de l'ASFC est le type de dépistage requis lorsque les fonctions ou les tâches d'un poste ou d'un marché nécessitent l'accès à des renseignements et à des biens désignés. Un individu accordée une cote de fiabilité peut avoir accès, au besoin de connaître, à des renseignements et biens désignés. Une cote de fiabilité de l'ASFC constitue la base nécessaire pour une cote sécuritaire Secrète ou Très secrète.

**Cote de sécurité** (Security clearance) – Indique que l'évaluation de sécurité a été complétée avec succès; avec un besoin de connaître, permet d'avoir accès à des renseignements classifiés. Il y a trois niveaux : confidentiel, secret et très secret.

**Couplage des données** (Data Matching) – activité qui consiste à comparer des renseignements personnels provenant de diverses sources, y compris de sources d'une même institution, à des fins administratives ou non administratives. Le couplage des données peut être systématique, récurrent ou peut être effectué périodiquement lorsqu'il est jugé nécessaire. En vertu de la Politique sur la protection de la vie privée, le couplage des données comprend la communication de renseignements personnels à une autre organisation à des fins de couplage de données.

**Courriel malveillant** (Malicious email) – message électronique, automatisé, contenant des fichiers en pièce jointe ou des hyperliens qui, si on clique dessus, peuvent permettre l'exploitation du système informatique et l'installation de logiciels nuisibles.

**Courrier recommandé** (Registered mail) – terme s'appliquant à l'envoi postal par lettre uniquement. Service postal qui est offert par Postes Canada ou des organismes équivalents de l'étranger et qui permet aux expéditeurs qui utilisent la poste aux lettres d'obtenir une preuve de dépôt de l'envoi et une attestation subséquente de sa livraison comportant la signature de son destinataire, son nom en lettres moulées et la date à laquelle l'envoi lui a été remis conformément aux normes et aux procédures en vigueur dans la région.

**Création de renseignements personnels** (Creation of personal information) - tout élément ou sous-élément de renseignements personnels qu'une institution fédérale attribue à un individu identifiable sans égard au fait que les renseignements proviennent de renseignements personnels existants dont

l'institution fédérale est responsable ou que l'institution fédérale appose de nouveaux renseignements au fichier de l'individu.

**Crise** (Crisis) - période de danger pour le gouvernement, du fait d'un sinistre, d'un désastre ou d'une malchance d'origine naturelle ou humaine. Pour qu'un événement soit considéré comme une crise, il n'est pas nécessaire qu'il constitue une grande menace pour la vie humaine, mais il doit porter atteinte, d'une manière ou d'une autre, aux convenances, aux traditions ou aux valeurs, à la sécurité ou à la protection du public, ou encore à l'intégrité du gouvernement.

**Critères de risque** (Risk criteria) – Cadre de référence grâce auquel un ministère définit et évalue l'importance des risques pour déterminer s'ils sont acceptables ou inacceptables.

**Crypto** (Crypto) - marque apposée à un matériel de chiffrement pour indiquer que ce matériel est assujetti à des contrôles particuliers régissant l'accès, la distribution, le stockage, la comptabilité, la disposition et la destruction.

**Cryptographique** (Cryptographic) – il s'agit communément de l'étude des moyens permettant de convertir l'information normale et lisible en format incompréhensible, pour la rendre illisible à quiconque n'a pas de connaissances secrètes pour la déchiffrer – c'est l'art du chiffrement.

**Cryptographie** (Cryptography) - discipline qui traite des principes, des moyens et des méthodes permettant de rendre des renseignements inintelligibles et de reconvertir des renseignements inintelligibles en renseignements cohérents.

– la cryptographie de type 1 est utilisée pour chiffrer les renseignements classifiés qui relèvent de l'intérêt national.

La cryptographie de type 2 est utilisée pour chiffrer les renseignements protégés ou de nature sensible qui ne relèvent pas de l'intérêt national.

**Cryptopériode** (Cryptoperiod) - laps de temps durant lequel une clé cryptographique est en vigueur.

**Cyberattaque** (Cyber attack) – tout accès, utilisation, manipulation, interruption ou destruction (par voie électronique) non intentionnel ou non autorisé d'information électronique et/ou d'infrastructures électroniques ou physiques qui servent au traitement, à la communication ou au stockage de cette information qui compromet la confidentialité, l'intégralité ou la disponibilité d'un ordinateur ou des réseaux et des renseignements qui sont accessibles par son intermédiaire.

**Cyberconférence** (Web conferencing) – participation à distance à une conférence ou à une réunion au moyen d'Internet ou de l'intranet.

**Cyberévénement** (Cyber event) – indique la possibilité d'une infraction ou d'une compromission d'un système, d'un service ou d'un réseau d'information, d'une violation d'une politique de sécurité de l'information ou d'une défaillance d'une mesure de protection.

**Cyberincident** (Cyber incident) – toute tentative non autorisée (réussie ou non) visant à accéder à un réseau ou à une ressource informatique (attaques informatiques, compromissions et contamination par virus), ou à le modifier, à le détruire, à le supprimer ou à le rendre non disponible.

**Cycle de mise à jour** (Update cycle) – concerne l'expiration des cotes de fiabilité ou des cotes de sécurité, qui sont accordées pour une période de 5 ou de 10 ans, selon le niveau. L'Agence doit mettre à jour la cote de fiabilité et les cotes de sécurité de niveau I (Confidentiel) et de niveau II (Secret) d'une personne tous les 10 ans. La cote de fiabilité + et la cote de sécurité de niveau III (Très Secret) doivent quant à elles être mises à jour tous les 5 ans.

**Cycle de vie** (Life cycle) – série d'étapes par lesquelles un document passe au cours de son existence. Ces étapes comprennent notamment la planification et l'analyse des besoins, la création, la collecte ou la réception, l'organisation, l'extraction, l'utilisation, l'accessibilité et la transmission, l'entreposage et la protection et l'élimination.

**Cycle de vie des biens** (Asset Life Cycle) – La vie d'un bien est décrite comme le point de création du bien, y compris tous les marchés conclus, jusqu'au point de mise hors service du bien qu'il soit perdu, volé, détruit, etc.

## D

**De nature non délicate** (Non-sensitive) – biens qui ne sont ni protégés ni classifiés.

**Déchiquetage** (Shredding) – méthode mécanique de coupe ou de broyage utilisée pour réduire en fragments des papiers d'épaisseur standard, des supports électroniques (disquettes, CD, DVD), des microfilms et des microfiches.

**Déclaration du cycle de vie** (Reporting life cycle) – cadre de la Direction générale des opérations utilisé par la Section de la gestion des urgences pour garantir que les recommandations faites à la suite des exercices, des événements ou des incidents sont traitées en priorité.

**Déclaration ou affirmation d'identité** (Identity claim) – déclaration ou affirmation de la véracité d'un renseignement concernant l'identité d'un client.

**Déclassement** (Downgrading) – réduction du niveau de classification (p. ex. de Secret à Confidentiel) de l'information ou du bien. La décision, consignée par écrit, de l'auteur des renseignements classifiés ou un autre magistrat habilité par l'administrateur général d'abaisser le niveau d'information de classification.

**Déclassification** (Declassification) – enlever la cote de sensibilité (niveau de classification) du renseignement ou du bien.

**Défaillance** (Deficiency) – défaut de satisfaire aux exigences liées à un contrôle de sécurité qui entraîne une exposition directe du personnel, des biens ou des activités à une compromission potentielle.

**Défaillance de l'infrastructure de communication** (Communication infrastructure failure) – interruption d'appareils, de services ou de programmes de télécommunication.

**Défaillance de l'infrastructure de données** (Data infrastructure failure) – défaillance du système de données de l'ASFC.

**Degré de certitude** (Assurance level) - Un niveau de confiance qui peut être invoqué par d'autres.

**Délégué** (Delegate) – cadre ou employé d'une institution fédérale délégué pour exercer les pouvoirs, attributions et fonctions du responsable de l'institution en vertu de la Loi.

**Délimitation** (Demarcation) – obstacles physiques identifiés autour de chaque zone dont l'accès est contrôlée.

**Délit d'action ou de commission** (Malfeasance) - désigne la commission d'un acte illicite, c.-à-d., un acte qu'une personne n'a pas le droit d'accomplir ou qu'un contrat, une loi ou un règlement lui interdit d'accomplir.

**Demande de renseignements personnels** (Privacy request) – demande de communication de renseignements personnels faite en vertu de la Loi.

**Démarche de prise en compte du risque** (Risk-informed approach) - pour la gestion intègre la gestion du risque aux structures de gouvernance et aux structures organisationnelles existantes, y compris à la planification des activités, à la prise de décisions et aux processus opérationnels. Elle fait également en sorte que le milieu de travail ait la capacité et les outils nécessaires pour innover tout en protégeant l'intérêt public et en préservant la confiance de la population.

**Déni de service** (Denial of service) – attaque pouvant empêcher l'utilisation des réseaux, des systèmes ou des applications.

**Dépendance** (Dependency) – le fait, pour un service, de dépendre de services, de biens et de ressources (y compris les particuliers) internes ou externes.

**Destruction** (Destruction) – suppression de renseignements ou de biens. La destruction accidentelle de biens peut survenir à la suite d'un incendie, d'une inondation, d'un tremblement de terre ou d'une autre catastrophe, mais peut aussi être le résultant d'une négligence ou d'un acte délibéré (p. ex. vandalisme, émeute, sabotage ou actes de guerre).

**Détection** (Detection) – utilisation des mécanismes, des systèmes et des procédures qui s'imposent pour signaler qu'il y a eu tentative d'accès non autorisé ou accès non autorisé.

**Détection de la fraude** (Fraud detection) – activités et techniques reconnaissant la présence d'activités frauduleuses passées ou en cours.

**Détournement** (Misappropriation) – désigne le détournement de fonds ou de biens à mauvais escient. Ce terme sert souvent, mais pas exclusivement, à décrire le détournement de fonds publics à des fins

personnelles ou autres; cependant, toute fin non autorisée par le Parlement constitue une forme de détournement.

Détournement de domaine (Pharming) - type commun de fraude en ligne qui consiste à diriger une personne vers un site malveillant et inapproprié en redirigeant l'adresse URL. Même si l'adresse URL est entrée correctement, une personne peut être redirigée vers un faux site.

**Diligence raisonnable** (Due diligence) (liée aux dossiers sur les pistes de vérification) – examen raisonnable des dossiers liés aux pistes de vérification permettant de garantir qu'ils correspondent à la charge de travail et aux tâches de l'employé.

**Disponibilité** (Availability)- condition d'être disponible et accessible de manière fiable et en temps opportun afin d'appuyer les opérations, les programmes et les services.

**Disponibilité d'accès** (Access availability) – fait en sorte que les utilisateurs légitimes ne se voient pas refuser indûment l'accès à des renseignements ou à des ressources.

**Dispositif de stockage amovible** (Removable media storage devices) - dispositif conçu pour être retiré de l'ordinateur au moment de la mise hors tension. Certains types de dispositifs amovibles peuvent être lus par des lecteurs et des pilotes de périphérique, tels que des disques optiques (CD, DVD) ou des cartes mémoire. Les dispositifs amovibles peuvent aussi désigner certains dispositifs de stockage amovibles qui sont utilisés pour transporter ou stocker des données, comme des cartes USB à mémoire flash ou des disques durs externes.

**Dispositif électronique personnel** (Personal electronic device) – tout appareil électronique détenu par l'employé (téléphones cellulaires, téléphones intelligents (iPhone, BlackBerry et autres), iPod, lecteurs MP3, appareils photo numériques, dispositifs Bluetooth, ordinateurs portatifs et autres).

**Dispositifs** (Devices) - outils utilisés pour recueillir, traiter, recevoir, afficher, transmettre, reconfigurer, balayer, stocker ou détruire l'information par voie électronique.

**Dispositifs d'accès Internet à haut débit** (Broadband internet access devices) – dispositifs permettant d'accéder à Internet au moyen d'une plus grande bande passante qui accélère la vitesse.

**Disposition** (Provision) – processus de coordination de la création de comptes d'utilisateur et d'autorisations d'accès à ces comptes.

**Divulgation** (Disclosure) – Communication de renseignements, par quelque moyen que ce soit, à une personne qui fait partie ou non du ministère responsable de l'information et qui n'est pas autorisée à accéder à cette information.

**Divulgation non autorisée** (Unauthorized disclosure) – divulgation interdite par la loi ou par des politiques gouvernementales ou ministérielles.

**Divulgation protégée** (Protected disclosure) - dDivulgation qui est faite de bonne foi par un fonctionnaire, selon le cas :

a) en vertu de la présente loi (Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles);

b) dans le cadre d'une procédure parlementaire;

c) sous le régime d'une autre loi fédérale;

d) lorsque la loi l'y oblige.

**Document** (Record) – représente tous les éléments d'information, quel qu'en soit la forme ou le support, à l'exception des publications. Les documents ont trait à de l'information qui a été créée, reçue et tenue par une organisation ou une personne, pour des raisons opérationnelles, des motifs liés aux obligations juridiques, ou pour s'acquitter de ces deux dernières responsabilités. Les documents comprennent également les enregistrements sonores, les bandes-vidéo, les films, les photos, les organigrammes, les cartes, les plans, les sondages et les données. Sont aussi compris tous les originaux, les copies et les ébauches des mêmes documents.

**Documents confidentiels du Cabinet** (Cabinet confidences) – les documents confidentiels du Cabinet sont mentionnés dans la Politique sur la sécurité des documents confidentiels du Cabinet (avril 2007) et comprennent, entre autres, les versions provisoires et finales des mémoires, les documents de travail, les ordres du jour et les avant-projets de loi.

Documents essentiels (Vital records) – documents irremplaçables ou dont le remplacement causerait un retard critique **pour les opérations.**

**Documents** importants (Important records) – documents dont le remplacement ou la reproduction engendre des inconvénients majeurs ou des dépenses importantes pour les opérations.

**Documents officielles** (Official records) – sont les documents qui on une valeur opérationnelle et qui rendent compte des activités du gouvernement ainsi que du processus décisionnel, p. ex. des documents financiers, des documents de planification et des documents de réunions.

**Documents utiles** (Useful records) – dossiers pouvant être remplacés ou reproduits sans que cela occasionne d'inconvénients ou de dépenses indus pour les opérations.

**Dommage et destruction** (Damage and destruction) – préjudice contre un bien ou une personne engendrant une perte de valeur ou d'utilité.

**Dossier d'accès électronique de l'employé** (Employee electronic access file) – dossier généré à des fins de contrôle de l'accès électronique à l'information douanière, par les employés, pour une période de temps précise.

**Droit d'accès minimal** (Principle of least privilege) – Un principe de base selon lequel le moins de privilèges possible devraient être accordés aux entités (personnes, processus, appareils) en fonction des tâches et des fonctions qui leur ont été confiées.

# E

**Effet adverse** (Detrimental effect) – perte ou dommage envers, ou subi par, toute personne ou objet.

**Élément local** (Local element) - personne inscrite auprès d'un compte COMSEC ou d'un sous-compte COMSEC qui peut recevoir du matériel COMSEC de ce compte.

**Employé** (Employee) - S'entend de toute personne travaillant pour l'ASFC, y compris les membres de la direction, les employés en congé sans solde, les stagiaires, les recrues et les étudiants, qu'ils soient nommés pour une période indéterminée ou déterminée, qu'ils soient des employés occasionnels ou à temps partiel ou qu'ils soient en détachement ou en affectation à l'ASFC.

**Employé essentiel** (Essential employee) – employé qui fournit des services essentiels.

**En contrepartie de** (Quid pro quo) – Ce terme veut dire « donnant, donnant ». Par exemple, un pirate compose des numéros de téléphone de façon aléatoire et prétend être un employé d'une entreprise qui rappelle pour offrir du soutien technique. Il finit par trouver quelqu'un qui a un vrai problème et qui est reconnaissant que quelqu'un le rappelle pour l'aider. Le pirate « aide » la personne à régler le problème et il lui demande d'entrer des commandes qui donnent au pirate un accès à l'ordinateur ou qui lancent un logiciel malveillant.

**Énoncé de sensibilité** (Statement of Sensitivity) – fournit une description détaillée du système ou de l'application à la fois un point de vue opérationnel et un point de vue technique. Il fournit également une liste des biens de valeur ou biens indispensables formant le système informatique avec une appréciation de la valeur de chaque bien du point de vue financier ou commercial.

**Enquête** (Investigation) – processus systématique et complet selon lequel on examine les circonstances entourant un incident ou une allégation en vue d'établir et de documenter tous les faits pertinents et d'en faire une analyse afin de permettre à la direction de prendre une décision éclairée.

**Enquête des Normes professionnelles** (Professional Standards Investigation) – S'entend de l'enquête officielle menée par un enquêteur des Normes professionnelles conformément aux lignes directrices relatives aux rapports et aux enquêtes des Normes professionnelles sur les cas présumés ou soupçonnés d'inconduite d'un employé et à l'examen de ces cas.

**Enquête sur les antécédents** (Background investigation) – enquête sur les antécédents d’une personne à des fins d’emploi, d’accès au crédit ou aux biens de nature délicate, entre autres.

**Enquêtes de sécurité sur le personnel** (Personnel security screening) – processus d'évaluation de la fiabilité des employés et de leur qualification professionnelle relativement à leur poste, ainsi que, lorsque l'intérêt national est en cause, de leur loyauté et fiabilité y afférant. Lorsque l'évaluation est satisfaisante, l'employé obtient une cote de fiabilité ou une cote de sécurité. La cote de fiabilité s'applique lorsque seulement des biens protégés sont en cause. Lorsque l'employé a accès à des biens classifiés, une cote de sécurité correspondant au niveau de nature délicate des biens en cause est décernée. Une cote de sécurité implique une cote de fiabilité préalable.

**Enquêteur** (Investigator) – S'entend de la personne autorisée par la Section des enquêtes relatives aux normes professionnelles de la Division de la sécurité du personnel et des normes professionnelles à enquêter à la suite d'une plainte déposée conformément aux lignes directrices.

**Enregistreurs de frappe** (Keystroke loggers) – Il s'agit d'un logiciel malveillant qui enregistre secrètement les frappes sur un clavier, de sorte que la personne qui utilise le clavier ne sait pas que ses activités sont surveillées.

**Entente de contrôle du matériel COMSEC comptable** (Accountable COMSEC material control agreement) – entente ayant force obligatoire conclue entre le Centre de la sécurité des télécommunications Canada et une entité (du gouvernement ou du secteur privé canadien) qui n'est pas mentionnée aux annexes I, I.1, II, IV et V de la Loi sur la gestion des finances publiques, qui autorise l'acquisition, la propriété, le contrôle et la gestion du matériel COMSEC. Elle prescrit également les conditions de financement, de revente et de disposition finale du matériel COMSEC.

**Entité** (Entity) – personne, groupe ou organisation clairement et uniquement identifiable. Une entité peut être un individu ou peut être un ministère fédéral, en fonction de l'étendue des besoins.

Entreprise (Business) – organisation se livrant au commerce de biens et/ou de services offerts aux consommateurs et qui est habituellement administrée dans le but de faire des bénéfices.

**Entrust** (Entrust) – entreprise internationale qui offre un logiciel de chiffrement de l'infrastructure à clés publiques appelé Entrust technologies. Entrust fournit aux entreprises et aux gouvernements des certificats numériques, un processus de sécurité d'infrastructure à clés publiques et un logiciel de chiffrement (logiciel de protection de gestion de l'identité).

**Enveloppe simple scellée** (Single sealed envelope) – enveloppe simple comportant l'adresse, sans cote de sécurité.

**Équipement COMSEC** (COMSEC equipment) - équipement et systèmes cryptographiques approuvés par le Centre de la sécurité des télécommunications Canada désignés pour protéger l'information et les données classifiées ou PROTÉGÉ C du gouvernement du Canada. Cet équipement peut également comprendre l'équipement auxiliaire cryptographique, l'équipement de production cryptographique et l'équipement d'authentification.

**Équipement de destruction** (Destruction equipment) – mécanisme ou processus servant à modifier le support contenant des renseignements protégés ou classifiés de manière à ce que ces renseignements ne puissent plus être lus ou extraits de ce support.

**Équipement de sécurité matérielle** (Physical security equipment) – pièces d'équipement, installations et éléments fonctionnels de construction conçus et utilisés pour refuser ou contrôler l'accès aux bien classifiés du gouvernement, p. ex. serrures, contenants, systèmes d'alarme et équipement d'élimination des rebuts classifiés. Comprend les systèmes auxiliaires indispensables au bon fonctionnement des pièces d'équipement, des installations et des éléments fonctionnels de construction.

**Espionnage par-dessus l'épaule** (Shoulder surfing) – en utilisant des techniques d'observation directe, tels que regardé par-dessus l'épaule de quelqu'un, pour obtenir des informations. L'Espionnage par-dessus l'épaule peut être utilisé pour obtenir une grande variété d'informations confidentielles. Soyez conscient de votre environnement lorsque vous travaillez sur ou affichez de l'information gouvernementale dans les espaces publics.

**État étranger** (Foreign state) − Tout autre État que le Canada.

**Étranger** (Foreign National) – personne qui n'a pas la citoyenneté canadienne ou le statut de résident permanent.

**Étude d'impact de la réglementation** (Regulatory impact analysis) – outil utilisé dans le cadre d'un changement réglementaire afin d'en évaluer l'impact sur l'environnement, la santé, la sécurité et le bien-être social et économique des Canadiens.

**Évacuation** (Evacuation) – déplacement immédiat et rapide de personnes visant à les mettre à l'abri de la menace ou de la présence d'un danger réel. Selon l'urgence, les évacuations peuvent être effectuées partiellement (seulement certains étages) ou complètement (tout l'immeuble).

**Évaluateurs** (Evaluators) – personnes affectées à un ou à plusieurs lieux (le cas échéant) afin de prendre des notes et d'évaluer le rendement d'une personne, d'une équipe ou d'une organisation en fonction des objectifs de l'exercice et des critères de rendement établis.

**Évaluation de la menace** (Threat Assessment) – évaluation de la nature, de la probabilité et des conséquences de divers actes ou événements qui sont susceptibles de faire courir des risques aux employés, aux informations et aux biens.

**Évaluation de la menace et des risques – Installations** (Facility Threat and Risk Assessment) – Il s'agit d'une évaluation de la menace et des risques effectuée à partir d'une liste des biens et renseignements classifiés ou désignés, propres à une installation existante ou projetée. On dresse également une liste des risques à l'égard d'autres biens conservés à l'intérieur de l'installation et des points faibles que présentent ces biens, en tenant compte des conditions prévalentes, avant de recommander des mesures destinées à pallier ces déficiences. Lorsque l'évaluation de la menace et des risques est utilisée pour l'élaboration de recommandations en matière de sécurité dans le cadre d'un projet de construction, les faiblesses observées peuvent permettre d'établir si les normes de sécurité pour cette institution peuvent efficacement contrer les menaces identifiées.

**Évaluation de la menace et des risques** (ÉMR) (Threat and Risk Assessment) – évaluation de la nature, de la probabilité et des conséquences de divers actes ou événements qui sont susceptibles de faire courir des risques aux employés, aux informations, aux biens et aux systèmes.

**Évaluation de la vulnérabilité** (Vulnerability Assessment) - processus visant à cerner et à évaluer les vulnérabilités, à estimer leur probabilité et leurs répercussions et à décrire toutes les mesures d'atténuation en vigueur s'y rapportant.

**Évaluation de sécurité** (Security assessment) − Conformément à l'article 2 de la Loi sur le SCRS, évaluation de la loyauté d'un individu envers le Canada et, à cet égard, de sa fiabilité.

**Évaluation des facteurs relatifs à la vie privée** (Privacy impact assessment) – processus d'élaboration des politiques permettant de déterminer, d'évaluer et d'atténuer les risques d'entrave à la vie privée. Les institutions fédérales doivent consigner et tenir à jour des évaluations des facteurs relatifs à la vie privée pour les activités et les programmes nouveaux ou modifiés qui utilisent des renseignements personnels à des fins administratives.

**Évaluation du risque** (Risk assessment) - évaluation de la probabilité qu'une lacune soit exploitée, d'après l'efficacité des mesures de sécurité existantes ou proposées.

**Évaluation tous risques** (All hazard risk assessment) – approche systémique pour identifier, analyser et évaluer en simultané les menaces et risques naturels, accidentels ou attribuables à des intentions malveillantes.

**Évaluation/analyse du risque** (Risk analysis / Evaluation) – L'analyse systématique des conditions, les actions et leur interaction qui constituent un risque particulier.

**Évaluations multi-institutionnelles des facteurs relatifs à la vie privée** (Multi-institutional privacy impact assessments) – évaluation des facteurs relatifs à la vie privée pour un programme ou une activité engageant plus d'une institution gouvernementale (voir la définition du terme Évaluation des facteurs relatifs à la vie privée).

**Événement** (Event) – activité qui se déroule à un endroit et à un moment prévus (p. ex. les sommets du G8 ou du G20 et les Jeux olympiques).

**Événement important** (Significant event) – événement, présent ou imminent, qui a un effet sur l'Agence et sa capacité d'assurer ses services indispensables (tiré du Cadre de gestion des évènements de l'ASFC).

**Examen de l'accès** (Access review) – processus qu'une organisation met en place afin d'assurer une vérification et un contrôle actifs de la pertinence de l'accès d'une personne aux systèmes et aux applications, établi en fonction du niveau minimal de compréhension nécessaire aux utilisateurs pour leur permettre d'accomplir ou de soutenir les activités ou les fonctions reliées à leur travail.

**Examen éthique et psychologique** (Psychological ethical testing) – évaluation de l'aptitude psychologique des employés et des nouvelles recrues à porter une arme à feu de façon sécuritaire et responsable pour l'Agence des services frontaliers du Canada (ASFC).

**Examen justifié** (Review for cause) – réévaluation de l'admissibilité d'une personne à détenir une cote de sécurité antérieurement octroyée. Il s'agit d'un processus officiel initié lorsque de nouvelles données susceptibles de remettre en question la fiabilité ou la loyauté de l'employé visé sont mises de l'avant ou signalées.

**Examen visuel** (Visual sweep) – examen qui peut se faire en quelques secondes en regardant autour de la zone immédiate afin de cibler tout élément qui sort de l'ordinaire ou toute menace non identifiée comme de la fumée dans un couloir.

**Examens de la sécurité technique** (Technical security reviews) – examens devant être effectués pour tous les réseaux, systèmes et applications des technologies de l'information (TI) de l'Agence en cours de développement ou de modification.

**Exercice** (Exercise) – occasion d'être formé et de s'exercer à assumer des rôles et des responsabilités lors d'un événement ou d'un incident majeur dans un contexte réaliste, mais exempt de tout risque. Plusieurs types d'exercices peuvent être menés, qu'il s'agisse de séminaires d'orientation, d'ateliers, d'exercices sur table, d'entrainements, d'exercices fonctionnels et d'exercices complets.

**Exercice complet** (Full-scale exercise) – exercice axé sur les opérations auquel participent toutes les capacités d'intervention d'urgence et requérant le déploiement complet du personnel et de l'équipement. Il s'agit d'une situation d'urgence simulée qui se rapproche le plus possible de la réalité.

**Exercice de préparation et simulation de sinistre** (Readiness exercises and disaster simulation) – mécanisme grâce auquel l'Agence peut tester et valider ses plans de gestion et ses cadres de communication des urgences en prévision d'une urgence.

**Exercice fonctionnel** (Functional exercise) - exercice axé sur les opérations qui se déroule en temps réel dans le cadre d'une mise en situation, sans toutefois nécessiter l'intervention du personnel ou du déploiement d'équipement. Ce type d'exercice est principalement axé sur la communication et la coordination durant un événement ou une urgence.

**Exercice sur table** (Table Top Exercise) – appelé également XT. Il s'agit d'une analyse animée en groupe visant à discuter d'une situation d'urgence, dans un contexte informel sans stress.

**Exigences de base** (Baseline security requirements) – dispositions ou mesures obligatoires devant être mises en œuvre et appliquées en tout temps. Ces contrôles sont établis en fonction d'une évaluation des risques et des mesures et promulgués sous la direction de l'agent de sécurité du ministère.

**Expert en la matière** (Subject matter expert) – personne ressource au sein d'une organisation qui possède l'expertise ou les connaissances spécialisées au sujet d'un programme, d'un secteur opérationnel ou d'une politique.

# F

**Faible préjudice** (Low degree of injury) - Se traduit habituellement par de l'embarras public, une perte financière peu importante, un dérangement dans les relations fédérales-provinciales ou internationales, et une perturbation sans gravité des activités gouvernementales internes entraînant des retards et des pertes de renseignements. Le service soutien le mandat de l'ASFC, mais il peut être rétabli dans le délai le plus long puisque son interruption n'a pas une incidence importante sur l'organisation.

**Falsification de documents** (Falsification of documents) – altération, destruction ou mutilation délibérée et frauduleuse d'un document visant à favoriser les intérêts privés d'un employé ou d'autres personnes.

**Famille** (Family) – conjoint ou conjoint de fait, enfants à charge (y compris du conjoint en droit ou du conjoint de fait), ou toute personne qui réside en permanence au domicile de l'employé ou avec qui l'employé réside de façon permanente; aux fins de cette politique, dans certaines circonstances, il peut être nécessaire d'inclure dans cette définition des membres de la famille qui ne résident pas avec l'employé.

**Faute d'exécution** (Misfeasance) – désigne l'accomplissement incorrect d'un acte licite.

**Faux-semblant** (Pretexting) – Cette expression désigne la création et l'utilisation d'un scénario inventé (le prétexte) pour susciter l'intérêt d'une victime ciblée de manière à accroître les chances que la victime divulgue de l'information ou pose des gestes malgré les réticences qu'elle aurait à le faire normalement.

**Fédération d'identité** (Identity federation) – groupe d'entités autonomes ayant fondé une collectivité reposant sur des relations de confiance dans le but de gérer l'identité de leurs clients.

**Fédération des justificatifs** (Federating credentials) – processus par lequel on établit une fédération dans laquelle les membres partagent des assurances de justificatifs avec des membres de confiance de la fédération.

**Fiches faisant autorité** (Authority cards) – ces fiches désignent les agents de l'ASFC à qui le président a conféré le pouvoir d'appliquer (ou de faire appliquer) certaines parties de la Loi sur les douanes et de la Loi sur l'immigration et la protection des réfugiés (LIPR). Exemple : agents chargés du renseignement, des enquêtes, de la vérification de l'observation, des audiences, de l'exécution de la loi dans les bureaux intérieurs.

**Fichiers de données et matériel contenant des renseignements** – (Data files/equipment containing information) - tout matériel (électronique ou sur papier) servant à stocker ou à consulter des renseignements (p. ex. clés USB, ordinateurs portatifs, CD-Rom, etc.).

**Filtrage** (Screening) – Le processus servant à contrôler les visiteurs et/ou le matériel aux points d'entrée d'une installation ou d'une zone d'accès restreint en vue d'autoriser l'accès.

**Filtrage de sécurité** (Security screening) – Processus consistant à mener une activité de filtrage de sécurité et à évaluer la fiabilité du particulier et sa loyauté envers le Canada à l'appui d'une décision d'accorder, d'accorder avec dispense, de refuser ou de révoquer une cote de fiabilité, une autorisation de sécurité ou une autorisation d'accès aux sites.

**Fins administratives** (Administrative purpose) – utilisation de renseignements personnels concernant un particulier « dans le cadre d'une décision le touchant directement ». Cela comprend toute utilisation de renseignements personnels visant à confirmer l'identité d'une personne (c.-à-d. à des fins d'authentification et de vérification) ainsi qu'à déterminer si celle-ci est admissible aux programmes gouvernementaux.

**Fins non administratives** (Non-administrative purpose) – est l'utilisation de renseignements personnels pour une fin qui n'est pas liée à une décision touchant directement la personne. Cela comprend l'utilisation de renseignements personnels à des fins de recherche, de statistique, de vérification et d'évaluation.

**Fonction de sécurité** (Security function) – Une activité qui appuie directement l'atteinte des objectifs du gouvernement en matière de sécurité, notamment des activités liées à la sensibilisation et à la formation en matière de sécurité, les enquêtes de sécurité sur des personnes, la sécurité matérielle (y compris la prévention de la violence en milieu de travail), l'information et la sécurité des technologies de l'information, la sécurité dans le cadre d'accords contractuels et non contractuels, la gestion des incidents de sécurité, la gestion de l'identité et la planification de la continuité des activités et la gestion globale de la sécurité dans un ministère ou un organisme ou à l'échelle du gouvernement.

**Fonction opérationnelle essentielle** (Critical business function) – fonction ou processus opérationnel particulier dont l'interruption engendrerait des répercussions majeures sur le personnel et les activités et nuirait au mandat et aux secteurs d'activités de l'Agence.

**Fonds public** (Public funds) – en matière de sécurité matérielle, « protection » désigne le recours à des obstacles matériels, psychologiques et de procédure visant à retarder l'accès non autorisé ou à exercer un effet dissuasif à cet égard, y compris les obstacles visuels et auditifs, l'argent servant à financer les titres d'État ou obtenu par la perception de l'impôt par une entité gouvernementale (p.ex. petite caisse, fonds dans une opération de caisse ou en transfert).

**Fonds publics** (Public money) – fonds publics appartenant au Canada, perçus et reçus par le receveur général ou un autre fonctionnaire public agissant en sa qualité officielle ou toute autre personne autorisée à en percevoir ou recevoir.

- les recettes de l'État;
- les emprunts effectués par le Canada ou les produits de l'émission ou de la vente de titres;
- les fonds perçus ou reçus pour le compte du Canada ou en son nom;
- tous les fonds perçus ou reçus par un fonctionnaire dans le cadre d'un traité, d'une loi, d'une fiducie, d'un contrat ou d'un engagement et affectés à une fin particulière précisée dans l'acte en question ou conformément à celui-ci.

**Formulaire de contrôle** (Security Control Form) - Les formulaires de contrôle servent à faire le suivi des déplacements des biens de sécurité contrôlés biens contrôlés aux fins de la sécurité ainsi que des incidents liés aux biens contrôlés aux fins de la sécurité.

BSF208 : Formulaire sur les biens contrôlés

BSF203 : Désignation du statut des échantillons d'impressions de timbres de point d'entrée

BSF152 : Rapport sur un incident relatif à la sécurité

BSF270 : Formulaire de départ ou de transfert d'un employé

BSF672 : Contrôle de l'utilisation quotidienne des timbres du point d'entrée.

**Fouille de poubelles** (Dumpster diving) – fouille des déchets générés par l'Agence par des personnes peu scrupuleuses qui tentent de s'approprier à des fins illégales des renseignements ou des biens.

**Fraude** (Fraud) – Désigne un acte intentionnel de tromperie, de manipulation ou de supercherie commis dans le but exprès de tirer un avantage injuste ou malhonnête ou de porter préjudice à une autre personne ou à une organisation. D'habitude, il y a fraude lorsqu'une personne cherche délibérément à se présenter sous un faux jour ou à cacher des faits importants afin d'inciter une autre personne à lui céder de l'argent ou quelque chose de valeur ou à renoncer à un droit légal.

**Fraude contre le gouvernement** (Fraud against government) – acte visant à tromper intentionnellement l'Agence afin d'obtenir un avantage indu ou illégal (financier, politique ou autre).

**Fraude d'identité** (Identity fraud) – usage trompeur de renseignements identificateurs d'une autre personne (vivante ou morte) dans le but de commettre diverses fraudes (y compris se faire passer pour une autre personne et utiliser frauduleusement les données d'une carte de débit ou d'une carte de crédit).

**Fraude Interne** (Fraud internal) – acte ou omission intentionnelle d'un employé pour son enrichissement personnel ou pour l'enrichissement d'un tiers au moyen de l'abus ou de l'application fautive délibéré des ressources, des recettes, des renseignements, des biens ou des pouvoirs de l'Agence des services frontaliers du Canada.

## G

**Gardien COMSEC** (COMSEC custodian) – Personne désignée responsable, par l'autorité COMSEC d'un ministère, de la réception, de l'entreposage, de la distribution, de la comptabilité, de la disposition et de la destruction de tout le matériel COMSEC porté au compte COMSEC du ministère, ainsi que de l'accès à ce matériel.

**Gardien COMSEC suppléant** (Alternate COMSEC custodian) – personne désignée par l'autorité COMSEC du ministère pour assister le gardien COMSEC et pour exercer les fonctions du gardien COMSEC durant l'absence temporaire de ce dernier.

**Gestion de l'identité et de l'accès** (Identity and access management) – terme courant décrivant le processus de gestion de l'accès aux ressources de l'entreprise. La définition de base est la suivante : ensemble des processus visant à gérer « qui a accès à quoi ». Les processus sont utilisés pour initier, enregistrer et gérer les identités des utilisateurs et les autorisations connexes d'accès aux renseignements détenus par l'ASFC, afin de fournir un accès adapté aux seuls employés qui en ont besoin et de limiter l'accès du personnel qui n'a pas besoin d'une ressource d'information précise.

**Gestion de la continuité** (Continuity management) –approche exhaustive globale visant à assurer la capacité de l'Agence à réaliser ses objectifs fondamentaux même si elle fait face à des situations difficiles. La gestion de la continuité suppose non seulement d'atténuer l'incidence des perturbations inattendues, mais aussi de garantir la capacité et la vitesse de l'organisation à se rétablir de façon efficace à la suite d'une urgence.

**Gestion de la continuité des activités** (Business Continuity Management) - Processus de gestion intégrée qui comprend l'élaboration et la mise en œuvre d'activités et qui assure la continuité ou le rétablissement des opérations et de la prestation de services indispensables en cas de perturbation (Sécurité publique Canada).

**Gestion de la sécurité des technologies de l'information** (Management of information technology security) – exigences sécuritaires que les ministères fédéraux doivent satisfaire pour assurer la sécurité de l'information et des biens de technologie de l'information (TI) placés sous leur contrôle.

**Gestion de l'identité** (Identity management) – ensemble des principes, pratiques, politiques, processus et procédures utilisés pour réaliser le mandat de l'organisation et ses objectifs liés à l'identité.

**Gestion de l'information** (Information management) – discipline qui oriente et appuie une gestion efficace et efficiente de l'information au sein d'un organisme, depuis l'étape de la planification et de l'élaboration des systèmes jusqu'à celle de l'élimination de l'information ou de sa conservation à long terme.

**Gestion des biens de sécurité contrôlés** (Security controlled asset management) – système de processus des contrôles internes qui fournit à l'ASFC l'assurance raisonnable que les éléments suivants sont réalisés : contrôle et comptabilité appropriés des biens contrôlés ; suivi et consignation fiables durant leur cycle de vie et respect des politiques, des lois et des règlements canadiens prescrivant les exigences garantissant le contrôle des biens

**Gestion des clés** (Key management) - procédures et mécanismes de génération, de distribution, de remplacement, de stockage, d'archivage et de destruction des clés, qui commandent les processus de chiffrement ou d'authentification.

**Gestion des demandes** (Request management) – processus d'interaction entre le milieu des affaires et les fournisseurs de services. Discipline liée au processus de gestion de toute demande, visant à permettre la présentation initiale, à fournir l'autorisation et à orchestrer le traitement.

**Gestion des incidents** (Incident Management) - processus en vertu duquel une organisation réagit lorsque survient un incident et contrôle celui-ci, en s'appuyant sur des plans ou des procédures dûment établis.

**Gestion des urgences** (Emergency management) – La gestion des situations d'urgence concernant une approche globale, incluant tous les dangers, y compris toutes les activités et les mesures de gestion des risques liés à la prévention et l'atténuation, la préparation, l'intervention et la récupération .

**Gestion du risque** (Risk management) - approche systématique permettant d'établir la meilleure marche à suivre en cas d'incertitude en définissant, en évaluant, en comprenant et en communiquant les questions liées aux risques, et en prenant des mesures à leur égard.

**Gestion du risque de sécurité** (Security Risk Management) – approche systématique employée pour évaluer les menaces, analyser les risques et mettre en œuvre les mesures de contrôle. Les principales étapes du processus comprennent la définition, l'évaluation et la gestion des risques en matière de sécurité.

**Gestion fédérée de l'identité** (Federation identity management) – partage « d'assurances de l'identité » avec des partenaires (membres) d'une fédération en qui l'on a confiance.

**Gestion intégrée des risques** (Integrated Risk Management) – démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques du point de vue de l'ensemble de l'organisation afin de favoriser la prise de décisions stratégiques qui contribuent à l'atteinte des objectifs globaux de l'organisation.

**Gestionnaire** (Manager) – S'entend d'un employé qui exerce un rôle de supervision ou de gestion, y compris un directeur.

**Gestionnaire régionaux de la sécurité** (Regional Security Manager) – personne qui s'est vu confier les responsabilités en matière de sécurité pour l'application des politiques, des procédures et des lignes directrices en matière de sécurité dans une région donnée.

**Gestionnaires à tous les niveaux** (Managers at all levels) – Cette expression désigne les superviseurs, les gestionnaires et les cadres supérieurs.

**Guide de sécurité de la conception** (Security design brief) – document dans lequel sont décrits les principes de base de la sécurité matérielle ainsi que les mesures de sécurité matérielle qui doivent être mises en œuvre pour chaque installation.

**Guide de sécurité du site** (Security site brief) – document dans lequel sont décrits les facteurs de sécurité matérielle dont il faut tenir compte au moment de choisir un nouvel emplacement pour l'installation.

**Guides d'accès fondés sur les rôles** (Role based access guides) –source faisant autorité servant à accorder les permissions minimales d'accès au système.

## H

**Hameçonnage** (Phishing) – forme de fraude par Internet faisant appel à de faux courriels, à de faux sites Web ou à d'autres sources d'information qui semblent authentiques dans le but de voler des renseignements de valeur comme des numéros de carte de crédit ou d'assurance sociale, des numéros d'identification et des mots de passe.

**Harcèlement** (Harassment) – S'entend de tout comportement qui rabaisse, embarrasse, humilie, importune, alarme ou agresse verbalement une personne et qui est jugé mal venu. Il peut s'agir de mots, de gestes, d'intimidation ou d'autres comportements inappropriés.

**Harcèlement criminel** (Stalking) – l'article 264 du Code criminel mentionne le « harcèlement criminel » et interdit à une personne d'adopter une conduite où elle harcèle une autre personne ou fait en sorte qu'une autre personne craigne raisonnablement pour sa sécurité – suivre une personne (ou une de ses connaissances) d'un lieu à un autre, sans qu'elle le veuille et de façon répétée; communiquer de façon répétée, directement ou indirectement, avec cette personne sans qu'elle le veuille; surveiller le domicile, le bureau, etc. de cette personne ou se comporter d'une manière menaçante à l'égard de cette personne ou d'un membre de sa famille. Généralement, il s'agit d'une conduite répétée durant une période qui cause à la personne harcelée une crainte raisonnable pour sa sécurité ou celle de ses proches ou connaissances.

**Hiérarchie des zones** (Hierarchy of zones) - Processus par lequel les ministères du GC doivent assurer l'accès au matériel COMSEC protégé et classifié et en assurer la protection en fonction d'une hiérarchie des zones clairement reconnaissable. Il y a cinq zones : zone d'accès public, zone d'accueil, zone de travail, zone de sécurité et zone de haute sécurité.

## I

**Identification** (Identification) – processus visant à reconnaître une entité ou un utilisateur désigné dans un système automatisé de traitement de l'information. En général, on utilise des noms uniques lisibles par machine.

**Identité** (Identity) – référence ou désignation utilisée pour distinguer une personne, une organisation ou un dispositif unique et particulier.

**Incapacité contractuelle** (Disability to contract) - la personne déclarée coupable d'une des infractions ci-après n'a pas qualité, après cette déclaration de culpabilité, pour passer un contrat avec Sa Majesté, pour recevoir un avantage en vertu d'un contrat entre Sa Majesté et toute autre personne ou pour occuper une fonction relevant de Sa Majesté :

a) toute infraction visée à l'article 121, 124 ou 418 (Code criminel);

b) toute infraction visée à l'article 380 (Code criminel) et commise à l'égard de Sa Majesté;

c) toute infraction visée à l'alinéa 80(1)d), au paragraphe 80(2) ou à l'article 154.01 de la Loi sur la gestion des finances publiques.

**Incertitude** (Uncertainty) – désigne l'état, même partiel, du manque d'information liée à la compréhension ou à la connaissance d'un événement, de ses conséquences ou de la probabilité qu'elle se produise.

**Incident complexe de sécurité des TI** (Sophisticated IT Security Incident) – événement habituellement déclenché par les auteurs d'une menace complexe qui est compliqué à détecter, dont il est difficile de se remettre, qui cause un préjudice aux réseaux et systèmes du gouvernement du Canada et qui porte atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information.

**Incident COMSEC** (COMSEC incident) - any occurrence that jeopardizes or potentially jeopardizes the security of classified or protected Government of Canada information while it is being stored, processed, transmitted or received during the telecommunications process.

**Incident de sécurité** (Security incident) – tout acte de violence en milieu de travail manifestée à l'endroit d'un employé ou tout acte, événement ou omission pouvant entraîner la compromission d'informations, de biens ou de services.

- Incident de sécurité critique (Critical Security Incident) – Incident qui peut avoir une incidence grave sur l'ensemble des fonctions de l'ASFC en causant des blessures graves ou la mort, d'importants dommages à la propriété, une perturbation partielle ou complète des opérations frontalières ou en posant une menace pour les services/opérations. Une mesure immédiate (signalement) est nécessaire pour atténuer les répercussions d'un tel incident de sécurité.
- Incident de sécurité non critique (Non critical Security Incident) – Incident de moindre ampleur qu'un incident de sécurité critique, mais qui peut quand même avoir des répercussions sur les opérations frontalières. Un tel incident de sécurité doit être signalé en temps opportun.

**Incident de sécurité des technologies de l'information** (Information technology security incident) – tout événement imprévu ou indésirable qui peut compromettre les activités d'exploitation ou la sécurité de l'information.

**Incident de sécurité non critique** (Non Critical Security Incident) - incident de moindre ampleur qu'un incident de sécurité critique, mais qui peut quand même avoir une incidence sur les opérations frontalières. Un tel incident de sécurité doit être signalé en temps opportun.

**Individus** (Individuals) – Employés occasionnels, employés nommés pour une période indéterminée, étudiants et employés contractuels.

**Information gouvernementale** (Government information) – information créée, reçue, utilisée et tenue à jour, peu importe sa présentation matérielle, et information préparée aux fins du gouvernement du Canada ou produite par celui-ci et considérée comme étant sous son contrôle dans le cadre de l'exécution de ses activités ou conformément aux obligations qui lui incombent aux termes des lois.

**Information sur la clientèle** (Client information) – tout type d'information sous quelque forme que ce soit provenant des clients ou les concernant obtenue ou créée par l'ASFC ou au nom de celle-ci, à l'exception des renseignements qui ne révèlent pas, directement ou indirectement, l'identité du client concerné, à moins qu'ils divulguent une profession, un secret industriel, commercial ou professionnel ou un procédé commercial.

**Infraction** (Violation) – S'entend d'un geste ou d'une condition (intentionnelle ou autre) qui entraîne le contournement d'un contrôle de sécurité ou une limitation de la capacité de répondre aux attentes de la direction en ce qui a trait à la gestion des risques relatifs à la sécurité matérielle.

**Infraction à la sécurité** (Breach of security) – un acte ou une omission, de façon délibérée ou accidentelle, qui compromet de façon réelle ou possible des marchandises contrôlées (conformément à la définition de la Partie 2 de la Loi sur la production de défense) ou la technologie connexe; ces infractions peuvent inclure les marchandises contrôlées ou la technologie perdue dans le transport; les marchandises contrôlées ou la technologie laissée dans un secteur non protégé auquel des personnes non autorisées ont accès; la divulgation non autorisée par toute personne; le vol; et la perte ou l'exposition à des circonstances qui font en sorte qu'il est probable qu'il y a eu une infraction à la sécurité.

**Infraction à la sécurité** (Security breach) - un acte ou une omission, de façon délibérée ou accidentelle, qui compromet de façon réelle ou possible des marchandises contrôlées (conformément à la définition de la Partie 2 de la Loi sur la production de défense) ou la technologie connexe; ces infractions peuvent inclure les marchandises contrôlées ou la technologie perdue dans le transport; les marchandises contrôlées ou la technologie laissée dans un secteur non protégé auquel des personnes non autorisées ont accès; la divulgation non autorisée par toute personne; le vol; et la perte ou l'exposition à des circonstances qui font en sorte qu'il est probable qu'il y a eu une infraction à la sécurité.

**Infraction à la sécurité des renseignements** (Breach of information) – acte ou événement qui pourrait compromettre ou qui a enfreint les mesures de protection destinées à assurer la confidentialité, l'intégrité et la disponibilité des renseignements, des systèmes et/ou des processus. Une infraction à la sécurité des renseignements peut avoir des répercussions sur la protection des renseignements personnels, les entreprises ou l'organisation.

- Renseignements personnels (Privacy) – renvoie à un incident de sécurité concernant les renseignements personnels.
- Entreprise (Business) – renvoie à un incident de sécurité concernant les renseignements d'une entreprise.
- Organisation (Organization) – renvoie à un incident de sécurité concernant les renseignements de l'Agence.

**Infraction punissable par mise en accusation** (Indictable offence) - infraction reprise dans la loi fédérale, justiciable uniquement par voie de mise en accusation et généralement considérée comme faisant partie des infractions criminelles les plus graves. Les poursuites par voie de mise en accusation constituent un processus judiciaire très long et complexe nécessitant des enquêtes préliminaires et des procès devant un juge ou un juge et un jury.

**Infrarouge** (Infared) – le rayonnement infrarouge est la radiation électromagnétique dont la longueur d'onde est plus grande que celle de la lumière visible mais plus courte que les rayonnements térahertz et les microondes.

**Infrastructure à clé publique** (ICP) (Public key infrastructure PKI) – système de chiffrement double visant à garantir la sécurité des transactions électroniques, à confirmer que la personne qui envoie le dossier électronique est bien celle qu'elle prétend et que le dossier électronique envoyé n'a pas été modifié par quelqu'un d'autre. L'ICP utilise des méthodes faisant appel à l'utilisation de signatures électroniques sécurisées pour assurer la validité et l'intégrité des dossiers électroniques. Comprend également un système de certificats numériques, des autorités de certification et diverses autorités d'enregistrement pour vérifier et authentifier la validité de toutes les parties concernées par une transaction sur Internet.

**Infrastructure critique** (Critical Infrastructure) – processus, systèmes, installations, technologies, réseaux, biens et services essentiels pour la santé, la sécurité et le bien-être des Canadiens ainsi que pour le fonctionnement efficace du gouvernement. Les infrastructures critiques (réseaux et systèmes) sont essentielles pour l'Agence : si elles ne fonctionnaient pas ou si elles étaient détruites, il y aurait d'importantes répercussions sur la prestation continue des services.

**Ingénierie sociale** (Social engineering) – fait de manipuler les autres et de gagner leur confiance afin de leur faire poser des gestes ou divulguer des renseignements de nature sensible. L'information obtenue et collectée peut alors être utilisée pour commettre une fraude ou pour fournir un accès non autorisé à des systèmes informatiques.

**Insigne d'accès** (Access badge) - document fourni par un ministère ou une organisation qui permet de reconnaître visuellement la zone, l'installation ou le complexe auquel le détenteur est autorisé à avoir accès. L'insigne d'accès ne doit pas être confondu avec la carte d'identité, car ils n'ont pas la même finalité ni le même aspect physique.

**Inspection** (Inspection) – vérification que tous les contrôles de sécurité sont en place comme exigé et que toutes les affirmations concernant ces contrôles sont justifiables.

**Inspection de sécurité** (Security inspection) – examen officiel de la mise en œuvre des politiques, des normes et des procédures.

**Installation** (Facility) – désigne un aménagement physique qui sert à une fin précise. On entend par installation une partie ou la totalité d'un immeuble, soit un immeuble, son emplacement et ses alentours, ou encore une construction qui n'est pas un immeuble. Le terme désigne non seulement l'objet même mais aussi son usage (p. ex., champs de tir, terres agricoles).

**Installation COMSEC** (COMSEC facility) - aire autorisée, située dans un immeuble ou un autre endroit, servant à la génération, au stockage, à la réparation ou à l'utilisation de matériel COMSEC.

**Installation secondaire** (Alternate facility) – endroit, autre que l'installation primaire, où on assure des services opérationnels, surtout pendant une urgence ou à la suite de celle-ci. Il s'agit d'un emplacement auxiliaire où les fonctions opérationnelles peuvent être exécutées lorsque les installations primaires sont inaccessibles.

**Insubordination** (Insubordination) – défaut ou refus de reconnaître l'autorité d'un supérieur ou de s'y soumettre.

**Intégrité** (Integrity) – état de ce qui est précis, complet, authentique et intact.

**Intégrité des logiciels** (Software integrity) – processus d'élaboration de logiciels ayant le moins de vulnérabilités possible.

**Intégrité professionnelle** (Professional Integrity) – les employés doivent exercer leurs pouvoirs en toute honnêteté, ouverture et équité, accepter la responsabilité de leurs gestes afin de bâtir et de préserver une réputation de confiance et de responsabilisation, traiter les autres de manière respectueuse, agir comme il se doit même quand personne n'est aux alentours et protéger les biens matériels et informationnels de l'ASFC.

**Interception illicite** (Eavesdropping) - écoute intentionnelle d'une conversation privée susceptible de révéler des renseignements pouvant compromettre l'information et les biens de l'Agence.

**Intérêt national** (National interest) – L'intérêt national se rapporte à des questions qui touchent la défense et le maintien de la stabilité sociale, politique et économique du Canada et, par conséquent, la sécurité de la nation. L'information qui pourrait nuire à l'intérêt national si elle était compromise est définie à certains articles particuliers de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, comme il est mentionné au point 2.1 de la Politique sur la sécurité.

**Interopérabilité** (Interoperability) – capacité des ministères et des organismes du gouvernement fédéral de fonctionner en synergie au moyen de pratiques uniformes en matière de gestion de la sécurité et de l'identité.

**Interruption** (Interruption) – La non-disponibilité d'un service. La mesure dans laquelle le service est essentiel aux opérations dicte l'importance de ce facteur en ce qui a trait au préjudice et à la menace.

**Interruption d'un service indispensable** (Critical service disruption) – interruption ou compromission d'un service indispensable sur le plan de la disponibilité ou de l'intégrité, qui pourrait avoir une incidence sur la capacité de l'Agence à exécuter son mandat de base. Voir « service indispensable ».

**Intervenants** (Players) – participants à un exercice qui exécutent les fonctions et les rôles qui leur sont attribués ou qui en discutent dans le cadre de l'exercice, en suivant les procédures d'intervention habituelles (à moins d'avis contraire). Ils agissent en fonction des renseignements que leur communiquent les autres participants et les simulateurs et prennent les mesures requises pour faire face à la situation d'urgence simulée et pour en atténuer les effets.

**Intervention** (Intervention) – mise en œuvre de mesures visant à faire en sorte que les incidents de sécurité soient déclarés aux responsables concernés et que des correctifs immédiats et à long terme soient apportés.

**Intervention - gestion d'urgence** (Response – emergency management) – Mesures prises pendant ou immédiatement avant ou après une catastrophe pour en gérer les conséquences et minimser la souffrance et les pertes.

**Intervention en TI** (Intervention en cas d'incident ou d'intrusion) (Response IT (incident response or intrusion response) – mesures prises en cas d'attaque ou d'intrusion pour protéger un système d'information et les données qu'il contient et rétablir les conditions de fonctionnement normales.

**Intimé** (Respondent) – désigne une personne contre laquelle une plainte est déposée.

Intranet (Intranet) – réseau informatique, notamment réseau basé sur la technologie d'Internet qu'une organisation utilise à l'interne, à des fins généralement privées et auquel les étrangers n'ont pas accès. Atlas est la page d'accueil de l'Agence des services frontaliers du Canada.

**Introduction par effraction** (Break and enter) – accès non autorisé à une installation à des fins criminelles.

**Intrusion** (Intrusion) – type d'incident lié à la sécurité des TI impliquant l'accès non autorisé à un système ou à un réseau, ou de l'activité sur celui-ci.

**Inventaire des risques** (Risk inventory) – processus visant à cerner, à reconnaitre et à consigner les risques.

## J

**Jeu** (Gambling) – parier, miser ou risquer de l'argent ou un article de valeur pour un jeu de hasard ou combinaison de jeu et d'habileté. Le jeu peut prendre de multiples formes, notamment les paris sportifs et les divers types de mises en commun.

**Journal de vérification** (Audit log) – fichier électronique généré par une application (Word, Excel, etc.) ou par un dispositif informatique ou de réseau. Ce fichier renferme des renseignements liés à la sécurité, tels que l'historique des accès (ouverture et fermeture de session), l'heure et les résultats des événements, entre autres données. Les journaux peuvent comporter un registre des activités de l'utilisateur et indiquer le résultat de ces activités, fournissant ainsi des données utiles aux activités judiciaires (p. ex. tentatives multiples d'authentification d'utilisateur).

**Justificatif d'identité** (Credential) – Objet (ou identificateur) physique ou électronique unique attribué à un client ou associé à celui-ci.

**Justificatifs anonymes** (Anonymous credential) – renvoie à un justificatif qui, tout en faisant une affirmation au sujet d'un bien, statut ou droit d'un client ne révèle pas l'identité du client. Un justificatif peut contenir des données relatives à l'identité, mais peut quand même être considéré comme anonyme si les données en question ne sont pas reconnues ou utilisées à des fins de validation de l'identité. Les justificatifs anonymes offrent aux clients la possibilité de prouver, dans l'anonymat, des déclarations les concernant ou portant sur leurs relations avec des organisations publiques ou privées.

## L

**Lieu de télétravail** (Telework place) – L'endroit où un employé et un employeur ont convenu que l'employé travaillera; il peut s'agir de la résidence de l'employé ou d'un autre endroit.

**Lieu de travail** (Workplace) – emplacement officiel où l'employé est affecté au départ.

**Ligne d'information pour les employés** (Employee Notice Line) La ligne d'information pour les employés de l'ASFC 1-866-668-4234 sert à obtenir des renseignements à jour sur les milieux de travail en cas de fermeture d'un immeuble. Exemples d'urgence ou de perturbation des opérations régulières : intempéries, catastrophes environnementales, urgences locales et nationales, manifestations ou occupations d'édifice.

**Ligne de conduite** (Security guidelines) – méthodes suggérées basées sur des pratiques exemplaires pour mettre en œuvre les politiques, normes et procédures de sécurité de l'Agence.

**Lignes directrices ministérielles sur la sécurité** (Departmental security guidelines) – méthodes préconisées pour mettre en œuvre les politiques, normes et procédures ministérielles. L'interopérabilité mondiale pour l'accès micro-ondes - technologie de télécommunication fournissant une transmission sans fil des données, par divers moyens, allant des liaisons point à point à l'accès intégral de type cellulaire mobile. Il s'agit d'une technologie fondée sur des normes qui permet l'accès sans fil à large bande du dernier kilomètre et offre une solution de rechange au câble et à la DSL.

**Liste de vérification relative à la sécurité** (Security Requirement Check List) – formule à l'usage des autorités de projet, des agents de sécurité ministériels, des agents d'approvisionnement ou d'autres fonctionnaires participant au processus contractuel en vue de recenser les exigences en matière de sécurité au début d'un processus contractuel ou précontractuel.

**Locataire majoritaire** (Major tenant) – locataire fédéral qui occupe la majorité de l'espace dans un immeuble.

**Locataire unique** (Sole Tenant) – dans les immeubles occupés seulement par un organisme ou un ministère fédéral, ce ministère est considéré comme étant le locataire unique. Dans de tels cas, le locataire unique assume toutes les responsabilités relatives aux urgences normalement dévolues au locataire majoritaire.

**Logiciel approuvé** (Approved software) – logiciel qui a été approuvé à l'avance ou certifié par l'ASFC/l'ARC/SPC pour les systèmes nationaux et locaux.

**Logiciel espion** (Spyware) – logiciel installé sur un ordinateur sans le consentement de l'utilisateur qui intercepte l'interaction de l'utilisateur avec l'ordinateur ou en prend le contrôle partiel. Généralement, les logiciels espions s'attaquent au navigateur Web (Internet Explorer) en faisant apparaître des fenêtres contextuelles ou des pages Web redirigées. L'infection peut se produire de diverses façons, notamment en ouvrant des pièces-jointes à des courriels, en cliquant sur des liens dans des pourriels ou en visitant des sites Web.

**Logiciels malveillants** (Malware) – Logiciel malveillant conçu spécifiquement pour endommager ou perturber un système, une attaque contre la confidentialité, l'intégrité et/ou de disponibilité. REMARQUE Les virus, vers informatique, chevaux de Troie, logiciel espion sont des exemples de logiciels malveillants.

**Logique cryptographique** (Cryptographic logic) - implémentation d'un ou de plusieurs algorithmes ainsi que d'alarmes, de contrôles et d'autres processus essentiels à l'exécution efficace et sécurisée de processus cryptographiques.

**Loi sur l'accès à l'information** (Access to Information Act) - Donne aux citoyens canadiens le droit de consulter l'information qui se trouve dans les dossiers de l'administration fédérale. La Loi est étroitement liée à la question de la sécurité, puisqu'elle sert de fondement législatif à la communication des renseignements gouvernementaux et aux exceptions sur ce plan.

**Loi sur la gestion des urgences** (Emergency Management Act) – explique comment prévenir et atténuer toute situation d'urgence nationale ou toute interruption des services essentiels qui pourrait avoir des conséquences sur la santé, la sûreté, la sécurité et le bien-être économique des Canadiens. Elle établit ce qu'il faut faire pour s'y préparer et les mesures à prendre pour assurer la reprise des activités. La sécurité est un aspect essentiel de l'élaboration des plans de continuité des activités.

**Loi sur la protection de l'information** (Security of Information Act) – Loi qui précise les sanctions applicables à tout comportement relatif à la sécurité des renseignements, comme l'espionnage, portant atteinte ou pouvant porter atteinte au Canada.

**Loi sur la protection des renseignements personnels** (Privacy Act) - protège la vie privée des personnes en fixant les règles entourant la collecte, l'utilisation, la conservation et le retrait des renseignements personnels au sein du gouvernement fédéral. La sécurité joue un rôle essentiel dans la protection des renseignements personnels contre la communication ou les usages non autorisés.

## M

**Mallette à documents approuvée** (Approved dispatch case) – Mallette approuvée par la GRC conçue spécialement pour le transport de renseignements protégés et/ou classifiés à bord de transporteurs commerciaux, et offrant une résistance adéquate contre les attaques subreptices dans cet environnement.

**Manifestation** (Demonstration) – groupe ou personnes qui organisent une manifestation à l'extérieur d'une installation de l'ASFC afin d'exprimer des opinions et d'exercer une pression politique.

**Manquement à la sécurité** (Violation of security) – désigne tout acte ou omission qui contrevient à une disposition des politiques sur la sécurité (PSG et ASFC).

**Manquement au devoir** (Neglect of Duty) – non-respect des lois, des règles et des politiques en vigueur ou des ordres donnés par les supérieurs dans l'exercice des fonctions.

**Manuel de sécurité** (ASFC) (Security manual) – série de politiques et de procédures normales d'exploitation soutenant la mise en œuvre de la Politique sur la sécurité du gouvernement diffusée par le Secrétariat du Conseil du Trésor (SCT).

**Matériel** (Material) – tout objet tangible, à l'exception des objets contenant des renseignements.

**Matériel à caractère violent** (Violent material) – comprend les documents qui représentent la violence physique, des actes ou des traitements violents.

**Matériel à contenu offensant** (Offensive material) – susceptible d'insulter, de dégouter ou de repousser. Comprend les blagues faites à l'encontre de groupes choisis (p. ex. plaisanteries raciales, religieuses ou sexistes) et peut aussi inclure les images à contenu offensant (p. ex. images de cadavres, de défécation).

**Matériel COMSEC** (COMSEC Material) – Matériel conçu pour sécuriser ou authentifier l'information de télécommunications. Le matériel COMSEC comprend, sans s'y limiter, les clés, l'équipement, les modules, les dispositifs, les documents, le matériel informatique, et les micrologiciels ou logiciels qui comportent ou décrivent une logique cryptographique et d'autres articles qui exécutent des fonctions COMSEC.

**Matériel COMSEC comptabilisé localement** (Locally-accountable COMSEC material) - matériel COMSEC auquel on a attribué un code de comptabilité 4 ou 7 et qui fait l'objet d'une comptabilité continue au sein d'un compte COMSEC après que celuici a envoyé le reçu initial au compte COMSEC distributeur.

**Matériel COMSEC comptable** (Accountable COMSEC material) – Matériel COMSEC qui nécessite un contrôle et une reddition de compte au sein du Système national de contrôle du matériel COMSEC (SNCMC) conformément à son code de comptabilité et dont le transfert ou la divulgation risquerait de porter préjudice à la sécurité nationale du Canada.

**Matériel cryptographique** (Cryptographic material) - tout le matériel, y compris les documents, les dispositifs et l'équipement, qui contient de l'information cryptographique et qui est indispensable au chiffrement, au déchiffrement ou à l'authentification des communications.

**Matériel de chiffrement** (Key material) - clé, code ou données d'authentification sur support physique ou électronique.

**Matériel personnel** (Personal equipment) – biens qui appartiennent aux employés (p. ex. argent liquide, caisse-café, vêtement ou autres articles personnels) *Bien que la perte et le vol de matériel personnel ne relèvent pas de la responsabilité de l'ASFC, ils peuvent révéler un problème au sein du bureau. Les incidents doivent être signalés au service local de sécurité.

**Mauvaise utilisation** (Misuse) – toute action ou inaction d'un utilisateur qui contrevient aux politiques, aux normes, aux procédures ou aux pratiques établies de l'ASFC ou constitue une activité inacceptable, illicite ou criminelle.

**Mauvaise utilisation des armes de service** (Misuse of duty firearm) – non-respect des politiques, des procédures ou des lignes directrices concernant l'utilisation des armes et de l'équipement de défense de l'Agence.

**Mauvaise utilisation des biens du gouvernement** (Misuse of government property) – le mésusage des biens de l'ASFC comprend l'utilisation de ces biens à des fins autres que celles relevant des activités officielles de l'ASFC. Les biens comprennent, sans s'y limiter, les véhicules, les immeubles, l'espace, les locaux, les installations, les uniformes, les fichiers et les documents, le matériel et les fournitures de bureau, les ordinateurs, les logiciels, le matériel vidéo, les dispositifs de télécommunication, les cartes de crédit du gouvernement et l'équipement de défense.

**Mauvaise utilisation des justificatifs** (Misuse of credentials) – utilisation de toute identification de l'ASFC de façon telle que l'on pourrait raisonnable croire qu'elle est faite pour en tirer un profit personnel, tenter d'exercer une influence indue ou obtenir, directement ou indirectement, une faveur, une récompense ou un traitement préférentiel pour soi ou d'autres personnes ou améliorer à mauvais escient sa propre image.

**Mauvaise utilisation des réseaux sociaux** (Misuse of social network) – utilisation des outils de médias sociaux susceptible de compromettre la réputation de l'Agence ou les relations de travail avec les collègues, les intervenants et les clients.

**Mauvaise utilisation des systèmes de TI** (Misuse of IT systems) – non respect des politiques, des procédures ou des lignes directrices concernant les systèmes de technologie de l'information, comprenant sans s'y limiter, l'utilisation des courriels, Internet, l'archivage de fichiers, l'accès aux bases de données détenues ou non par l'ASFC et aux données qu'elles contiennent.

**Mauvaise utilisation du système de courriel de l'ASFC** (Misuse of CBSA e-mail system) – utilisation du système de courriel de l'Agence pour se livrer à des activités criminelles, illicites et inacceptables.

**Mémoire officielle des identités** (Authoritative identity store) – la source faisant autorité ou le dispositif de stockage d'identité est la source de données transmises dans le système de gestion de l'identité. Il s'agit simplement d'un répertoire ou d'une base de données qui contient les renseignements sur l'identité d'une personne. Généralement, la source faisant autorité contient des renseignements comme l'identification de l'employé, le prénom, le nom, le numéro de téléphone, le courriel, le ministère, etc.

**Menace** (Threat) – événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux employés, aux renseignements, aux biens ou aux services.

**Menace complexe à la sécurité des TI** (Sophisticated IT security threat) - entité qui recourt à des technologies de pointe et à des procédés perfectionnés pour pénétrer ou contourner des systèmes de protection et des technologies de sécurité sans être décelée.

**Menace de l'intérieur** (Insider Threat) - Toute personne (employe, entrepeneur, etc.) ayant un accès autorisé qui, intentionnellement ou non, porte atteinte aux intérêts d'un organisme.

**Menaces envers la sécurité du Canada** (Threats to the security of Canada) – constituent des menaces envers la sécurité du Canada les activités suivantes :

a) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage;

b) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque;

c) les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique, religieux ou idéologique au Canada ou dans un État étranger;

d) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence. La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas a) à d).

**Mention article cryptographique contrôlé** (Controlled cryptographic item marking) - marque apposée à un matériel COMSEC pour indiquer que ce matériel est assujetti à des exigences spéciales en matière de traitement et de contrôle.

**Mention(s) de sécurité** (Security marking(s)) – Mentions ou métadonnées cohérentes et acceptées qui sont appliquées à l'information ou aux biens afin de communiquer la catégorie et le niveau de sensibilité de l'information ou des biens.

**Mesure de protection accrue** (Enhanced safeguard) – niveau de sécurité excédant les normes de base acceptées (voir aussi Sécurité accrue).

**Mesure de protection administrative** (Administrative safeguard) – application des politiques, directives, règles, procédures et processus écrits d'une institution gouvernementale ayant trait à la protection des renseignements personnels tout au long du cycle de vie tant des renseignements personnels que du programme ou de l'activité.

**Mesure de protection de base** (Minimum safeguard) – dispositions obligatoires du programme de sécurité, établies en fonction de la Politique sur la sécurité du gouvernement ainsi que des normes connexes et des exigences techniques s'y rapportant (voir également le terme Exigences de base).

**Mesure de protection physique** (Physical safeguard) – installations et équipement qui servent à protéger le système de soutien où sont enregistrés et conservés les renseignements personnels.

**Mesure de protection technique** (Technical safeguard) – mesures de la technologie de l'information utilisées pour protéger les installations, l'équipement et le système de soutien où les renseignements personnels sont enregistrés et conservés.

**Mesures de protection** (Safeguards) – moyens approuvés et mis en œuvre pour assurer la confidentialité, l'intégrité, la disponibilité et l'authenticité de l'information et la protection des employés et des biens; les moyens sont normalement définis par l'entremise d'un processus de gestion du risque.

**Mesures de protection progressives** (Graduated safeguards) – ensemble de mesures de protection, de niveau de sécurité croissant, qui réduisent respectivement le risque.

**Méthodes de contrôle d'accès** (Access control methods) – méthodes utilisées pour prévenir l'accès non autorisé. Ces méthodes peuvent comprendre des systèmes faisant intervenir des êtres humains, soit des gardiens ou des réceptionnistes, des systèmes fondés sur les caractéristiques physiques (p. ex. empreintes digitales ou signatures) ou basés sur des dispositifs de contrôle de l'accès, comme des clés ou des cartes de proximité.

**Ministère** (Department) – Tous les ministères énumérés à l'annexe I, toutes les divisions ou directions générales de l'administration publique fédérale nommées dans la colonne I de l'annexe I.1, les sociétés nommées à l'annexe II et les entités de l'administration publique fédérale nommées aux annexes IV et V de la Loi sur la gestion des finances publiques (LGFP), à moins qu'elles soient exclues par des lois, des règlements ou des décrets particuliers.

**Ministère gardien** (Custodian department) – ministère responsable de l'administration d'un immeuble attribué à d'autres ministères au titre de l'exécution de programmes gouvernementaux. Pour l'Agence, il peut s'agir de l'Agence elle-même (en termes de propriété détenue), des Travaux publics et Services gouvernementaux Canada ou d'une entité privée. Dans le contexte de la sécurité des installations, le lien particulier entre ces deux entités est défini dans le cadre de l'Accord d'occupation.

**Mise en garde** (Caveat) – cote indiquée en plus du niveau de confidentialité qui indique les limites relatives à l'accès ou les mesures particulières de manipulation.

**Modification** (Modification) – dénaturation ou altération de l'information, des données, des logiciels, des systèmes ou du matériel informatique. Il est souvent difficile de confirmer la dénaturation ou l'altération des données ou des programmes, surtout quand ils sont lisibles par machine.

**Mot de passe** (Password) – il s'agit d'une chaîne de caractères (c'est-à-dire les lettres, les chiffres et autres symboles) utilisés pour authentifier l'identité ou pour vérifier l'autorisation d'accès. Il est utilisé en combinaison avec un nom d'utilisateur pour accéder à un poste de travail, une application, un service en ligne ou un serveur de réseau.

## N

**Naturel** (Natural) – Comme l'indiquent diverses bases de données sur la gestion des urgences, des services météorologiques, l'Organisation mondiale de la santé et des organisations de voyage (en particulier la flore et la faune).

**Négligence** (Negligence) – désigne une action ou omission qui résulte en une perte de fonds ou en des dommages matériels en raison d'un manque de soins adéquats et raisonnables.

**Nettoyer** (Sanitized) – se dit des données purgées des informations personnelles identifiables afin de protéger la vie privée des utilisateurs.

**Niveau d'assurance des justificatifs** (Credential assurance level) − Le niveau d'assurance qu'une personne, une organisation ou un appareil a conservé le contrôle de ce qui lui a été confié (p. ex. clé, jeton, document, identificateur) et que le justificatif n'a pas été compromis (p. ex. falsifié, corrompu, modifié).

**Niveau d'assurance de l'identité** (Identity assurance level) − Le niveau d'assurance que la personne, l'organisation ou l'appareil est bien celui qu'il prétend être.

**Niveau de services minimal** (Minimum service level) – niveau de prestation des services qui s'avère essentiel pour éviter un préjudice important. Ce niveau est maintenu jusqu'à ce que le rétablissement soit complet.

**Niveaux de préparation** (Readiness levels) – Les niveaux de sécurité accrue qui doivent être appliqués dans les installations du gouvernement du Canada en cas d'urgence ou lorsqu'il y a des menaces plus importantes.

**Non-répudiation** (Non-repudiation) – les services de non-répudiation offrent à l'utilisateur une protection contre un autre utilisateur qui pourrait nier par la suite qu'un échange de communication a eu lieu. En général, la preuve de non -doit se révéler convaincante pour un arbitre tiers.

**Normes de sécurité** (Security Standards) – exigences obligatoires détaillées en matière de sécurité (tirées des politiques sur la sécurité) élaborées par la Direction de la sécurité et des normes professionnelles.

**Nudité** (Nudity) – personne nue ou qui montre ses organes génitaux. Acte qui n'est pas nécessairement à caractère sexuel.

# O

**Objectif de délai de rétablissement** (Recovery time objective) – période de temps à l'intérieur de laquelle les systèmes, les applications et l'infrastructure doivent être rétablis à la suite d'une catastrophe.

**Objectif de l'exercice** (Exercise goal/objective) – ce que l'exercice vise à accomplir (p. ex. cerner les lacunes en matière de planification, discuter des exigences en matière de rapports, accroître les connaissances quant aux rôles de chaque ministère).

**Objectif de point de rétablissement** (Recovery point objective) – moment jusqu'auquel les données doivent être récupérables pour que cela soit acceptable pour le propriétaire des processus que soutiennent les données.

**Objectif des contrôles de sécurité** (Security Control Objective) – s'entend de l'énoncé des résultats ou des buts que l'on souhaite atteindre en mettant en place de tels contrôles.

**Objectifs de sécurité** (Security goals) – les objectifs de sécurité correspondent à l'état qui survient lorsque les objectifs des contrôles de sécurité fonctionnent comme prévu en vue de maintenir un niveau bien déterminé de risque résiduel. Objectifs en matière de contrôles de sécurité : Ce terme est décrit à l'annexe C de la Directive sur la gestion de la sécurité ministérielle, publiée par le Secrétariat du Conseil du Trésor du Canada. Il s'agit d'énoncés des résultats escomptés ou des objectifs à atteindre en mettant en œuvre des contrôles de sécurité (adaptation des Objectifs de contrôle de l'information et des technologies associées).

**Observateur** (pour la gestion d'urgences ou exercices PCA) (Observer for EM or BCM) - participants qui ne sont ni des intervenants ni des agents de confiance. Les observateurs sont témoins des événements liés aux exercices.

**Observateur** (pour les Enquêtes relatives aux normes professionnelles) (Observer for Professional Standards Investigation) – S'entend d'un employé qui n'est ni un témoin dans le cadre d'une enquête des Normes professionnelles ni un représentant syndical, et qui est invité par le répondant et autorisé par l'enquêteur à assister à l'entrevue du répondant par l'enquêteur.

**Observation** (Observation) – problème qui a pu être observé durant la tenue d'un exercice, d'un événement ou lors d'un incident.

**Occupation** (Occupation) – se dit lorsqu'un groupe ou des personnes occupent des lieux et refusent d'en sortir afin d'exprimer des opinions et d'exercer une pression politique.

**Omission délictueuse** (Nonfeasance) - désigne l'action d'omettre totalement ou de négliger d'accomplir un acte ou une tâche ou d'exécuter un engagement lorsqu'il y a obligation d'agir.

**Opérations pyramidales** (Pyramid schemes) – systèmes hiérarchiques qui encouragent à envoyer de l'argent dans l'espoir qu'un nombre fixe de personnes vous en enverront à leur tour.

**Opportun** (Timely) – se dit d'un élément effectué ou ayant lieu à un moment favorable ou en temps utile. En contexte d'évaluation des risques, pour être considéré comme étant opportun, l'élément étudié doit être examiné en fonction des opérations, des menaces et de l'environnement existants, et il ne doit pas y avoir de changement majeur concernant l'information pertinente.

**Ordre de mission de messager COMSEC** (COMSEC courier certificate) – document autorisant le porteur à transporter du matériel COMSEC.

**Outils Web 2.0** (Web 2.0 tools) - Outils et services Internet qui permettent l'échange d'informations, le dialogue et la production de contenu par l'utilisateur. Cela peut comprendre les médias sociaux et les technologies de collaboration.

## P

**Pandémie** (Pandemics) – épidémie d'une maladie infectieuse qui s'est répandue dans les populations humaines de l'ensemble d'une vaste région; par exemple, sur plusieurs continents ou même à l'échelle de la planète.

**Pare-feu** (Firewall) – équipement matériel ou logiciel qui contrôle l'accès interne et externe à un sous-réseau. Un pare-feu examine (filtre), selon un ensemble de règles, tout paquet de données qui tente d'entrer ou de sortir d'un réseau et décide si le paquet peut être accepté.

**Parenté** (Relative) – désigne toute personne faisant partie d'une catégorie de personnes unies par les liens du sang, du mariage ou de l'adoption, par une union de fait ou tout autre type de lien juridique.

**Passage en double** (Piggybacking) - l'entrée par passage en double signifie qu'une personne suit un employé autorisé pour passer un point de contrôle ou une porte, sans que le système effectue une vérification. Selon les circonstances, cette méthode est inacceptable et peut être légale ou non, autorisée ou non.

**Passage en double** (Tailgating) – Un individu tente d'entrer dans une zone réglementée en suivant une personne qui a un accès légitime à cette zone. Voulant faire preuve de simple courtoisie, la personne autorisée tient habituellement la porte pour l'individu. La personne autorisée peut omettre pour une raison quelconque de demander à l'individu de lui montrer une pièce d'identité ou peut supposer que l'individu a oublié ou perdu le jeton d'identité nécessaire. L'individu peut aussi présenter un faux jeton d'identité.

**Passe-partout** (Master key) – clé unique qui ouvre toutes les serrures à clés identiques ou différentes reliées à ce passe-partout.

**Périmètre** (Perimeter) – limites extérieures d'un site.

**Permanent** (Continuous) – ne doit pas être interrompu.

**Permissions d'accès minimal aux systèmes** (Minimum system access permissions) – besoin d'une personne de n'avoir que les accès nécessaires pour pouvoir exercer ses fonctions.

**Permissions d'accès privilégié aux systèmes** (Privileged system access permissions) – désigne l'autorisation ou l'ensemble des autorisations qui permettent aux utilisateurs de contourner les

contrôles d'accès logiques et d'exécuter les fonctions qui sont habituellement interdites à des utilisateurs ordinaires (non privilégiés).

**Personnel clé** (Key personnel) – personnes au sein d'une équipe de gestion de la continuité qui jouent un rôle clé dans le processus de continuité et de rétablissement. Le personnel clé aura une bonne compréhension du service indispensable et de ce qui est nécessaire pour rétablir le service.

**Personnes autorisées** (Authorized users) - personnes travaillant avec le gouvernement du Canada, y compris les employés occasionnels, les entrepreneurs, les étudiants et autres personnes qui ont été autorisées par l'administrateur général à accéder aux dispositifs et réseaux électroniques du gouvernement du Canada.

**Personnes ayant besoin d'aide** (Persons requiring assistance) – personnes qui ne peuvent pas évacuer les lieux en toute sécurité sans assistance en raison d'une blessure, d'une maladie, d'une déficience ou d'un problème médical permanent ou temporaire. Ces personnes doivent s'auto-identifier auprès de leur gestionnaire/superviseur et de l'organisation de secours de l'immeuble.

**Perte** (Loss) - un article est considéré comme étant « perdu » lorsque le propriétaire ne l'a plus en sa possession ou n'a plus la garde de celui-ci, malgré lui et par quelque moyen que ce soit, mais plus particulièrement par accident, négligence ou par oubli, et quand il ne sait pas où il se trouve ou ne peut pas le récupérer par une recherche diligente courante.

**Pertinent** (Relevant) – clairement lié à la question en jeu ou approprié.

**Perturbation** (Disruption) – toute interruption qui compromet la prestation continue des services essentiels de l'Agence et leur intégrité.

**Pièce sécuritaire** (Secure room) – Pièce totalement close pourvue de dispositifs de sécurité et destinée à l'entreposage de biens de valeur et permettant de les protéger contre des menaces précises.

**Piratage** (Hacking) − Terme utilisé pour décrire des actes posés par quelqu'un pour accéder à un ordinateur sans autorisation. La disponibilité d'une ligne d'information sur les outils, les techniques et les programmes malveillants fait en sorte qu'il est facile, même pour des gens qui ne sont pas spécialistes, de mener des activités malveillantes.

**Pirate informatique** (Hacker) - personne qui utilise ses compétences en programmation et sa connaissance des systèmes pour obtenir un accès non autorisé à un ordinateur ou à un réseau.

**Piste de vérification** (Audit trail) - enregistrement chronologique des activités d'un système permettant de reconstituer et d'examiner la séquence des événements ou des changements survenus dans un événement (ou les deux).

**Plaignant** (Complainant) – individu alléguant l'inconduite d'un employé.

**Plainte** (Complaint) –. S'entend d'une allégation ou d'une suspicion d'inconduite par un employé.

**Plan d'action pour l'amélioration** (Improvement action plan) - Documents sous forme de tableau, qui souligne les observations et les recommandations reprises dans le Compte Rendu PostAction/Compte Rendu Post Événement/Compte Rendu Post Incident, en vue de faciliter le suivi de l'application des recommandations.

**Plan d'intervention** (Response Plan) - plan d'urgence qui décrit les mesures et les procédures s'appliquant à la phase d'intervention d'un événement.

**Plan d'action en cas d'incident** (Incident action plan) – Comporte des objectifs qui tiennent compte de la stratégie globale en matière d'incidents et des mesures tactiques et des renseignements à l'appui précis pour la prochaine période opérationnelle.

**Plan de continuité des activités** (Business continuity plan) – plan qui fournit l'information requise pour minimiser l'impact d'une interruption de service et qui dresse la liste des stratégies à adopter afin d'assurer une reprise efficace et en temps opportun des opérations à la suite d'une interruption majeure des activités.

**Plan de reprise après catastrophe** (Disaster recovery plan) - ententes, processus, procédures et activités approuvés visant à faire en sorte, à la suite d'une catastrophe, que les systèmes d'application de la TI, les données et l'infrastructure recouvrent des niveaux opérationnels acceptables pour une organisation donnée.

**Plan de sécurité du ministère** (Departmental security plan) - plan qui précise les décisions en matière de gestion des risques liées à la sécurité et définit les stratégies, les buts, les objectifs, les priorités et les échéanciers établis pour améliorer la sécurité de l'Agence et soutenir sa mise en œuvre.

**Plan de sécurité en cas d'incendie** (Fire safety plan) – composante du plan d'intervention en cas d'urgence (PIU) qui prévoit l'information et fournit les procédures d'intervention d'urgence directement liées aux incendies.

**Planification de la continuité de la gestion de l'information** (GI) (Information management (IM) continuity planning) - en tant que partie intégrante du Programme de planification de la continuité des activités et en conformité avec la Politique de gestion de l'information gouvernementale, la planification de la continuité de la GI consiste à élaborer des plans, des mesures, des procédures et des préparatifs (en se fondant sur la méthode de PCA pour garantir que les services et biens essentiels en GI sont toujours disponibles ou interrompus pendant de très brèves périodes.

**Planification de la continuité de la technologie de l'information** (TI) (Information technology (IT) continuity planning) – La planification de la continuité de la technologie de l'information (TI) identifie les missions services informatiques critiques, les données, les réseaux, les systèmes et les ressources nécessaires aux services essentiels et comprend l'élaboration des plans, des mesures, des procédures et des arrangements (à l'aide de la méthodologie PCA) de sorte qu'il y ait peu ou pas d'interruption dans la disponibilité des services informatiques critiques et les biens.

**Planification de la continuité des activités** (Business continuity planning) - Les produits ou services essentiels sont ceux que doit fournir une organisation pour assurer la survie, pour éviter de causer des blessures et pour respecter ses obligations juridiques ou autres. La planification de la continuité des activités est un processus de planification proactif qui assure la prestation des services ou des produits essentiels lors d'une interruption.

Un plan de continuité des activités (PCA) comprend :

• des plans, des mesures et des dispositions assurant la prestation continue de services et de produits essentiels, ce qui permet à l'organisation de recouvrer ses installations, ses données et ses biens;

• la détermination des ressources nécessaires pour soutenir la continuité des activités, dont le personnel, l'information, l'équipement, les ressources financières, les conseillers juridiques, la protection de l'infrastructure et les locaux.

**Planification de la gestion des urgences** (Emergency management planning) – processus d'élaboration, de validation et de mise à jour des plans, des politiques et des procédures liées à la gestion des urgences.

**Plans de gestion des urgences** (Emergency management plans) – plans élaborés pour assurer la sécurité et le bien-être des employés en cas d'urgence qui expliquent les procédures à suivre afin de rétablir efficacement les services indispensables à la suite d'une urgence. Ceux-ci comprennent le plan de gestion de la continuité (PGC), le plan d'intervention en cas d'urgence (PIU) et le plan de sécurité en cas d'incendie (PSI).

**Plate-forme** (Platform) – ordinateur, y compris le matériel, le système d'exploitation et l'infrastructure connexe liés à un réseau informatique servant à traiter, à recueillir, à transmettre ou à stocker de l'information.

**Politique de sécurité** (Security policy) – cadre qui précise les exigences obligatoires en matière de sécurité de l'Agence fondées sur la Politique sur la sécurité du gouvernement. Il s'agit des règles, des directives et des pratiques conçues pour assurer la protection du personnel, des renseignements et des biens.

**Politique de sécurité du ministère** (Departmental security policy) – exigences génériques de sécurité obligatoires élaborées et promulguées par la Direction de la sécurité et des normes professionnelles.

**Politique sur la sécurité du gouvernement** (Policy on government security) – politique aidant à protéger les employés et les biens du gouvernement; y sont décrites les mesures de protection essentielles à la réduction des risques de préjudice découlant de diverses menaces.

**Pornographie** (Pornography) – désigne les documents présentant du contenu sexuel explicite conçus ou prévus pour causer l'excitation sexuelle.

**Possibilité d'amélioration** (Opportunity for Improvement) – défaut de satisfaire aux exigences liées à un contrôle de sécurité SANS exposer directement un bien à une compromission potentielle.

**Pour cause** (For cause) – Détermination d'une raison valable d'examiner, de révoquer, de suspendre ou de déclasser une cote de fiabilité ou de sécurité, ou un accès à un site. Dans le cadre d'une évaluation de sécurité, détermination de la pertinence de vérifications plus approfondies.

**Pourriels** (Spam messages) – courriels provenant d'une adresse externe, qui ne sont pas souhaités et qui n'ont pas été sollicités. La plupart des pourriels sont envoyés à des fins publicitaires mais certains peuvent être des messages à contenu criminel (pornographie infantile et escroqueries).

**Praticiens de la sécurité** (Security practitioners) – personnes responsables de la coordination, de la gestion et de la prestation de conseils et de services relatifs aux activités de sécurité qui s'inscrivent dans un programme de sécurité ministérielle coordonné, notamment la sécurité de la technologie de l'information (TI), la sécurité matérielle, les enquêtes de sécurité sur le personnel, la gestion des urgences, la planification de la continuité des activités et les opérations de sécurité régionales.

**Pratique exemplaire** (Best practice) - méthode servant à gérer le risque en matière de sécurité d'une manière qui satisfait à toutes les exigences, sans être efficace de manière inhabituelle ou distincte.

**Pratiques et contrôles de gestion** (Management practices and controls) – politiques, processus, procédures et systèmes qui permettent à un ministère de mettre en œuvre ses programmes et ses activités, d'utiliser ses ressources de façon efficace, de pratiquer une saine gérance, de respecter ses obligations et d'atteindre ses objectifs.

**Pratiques relatives à la protection de la vie privée** (Privacy practices) – toutes les pratiques relatives à la création, la collecte, la conservation, l'exactitude, l'utilisation, la divulgation et le retrait des renseignements personnels.

**Pré-enquête** (Preliminary Inquiry) – fait d'obtenir, auprès de la personne qui a formulé une allégation, tous les détails possibles relativement aux faits et aux circonstances dénoncés, de vérifier la documentation disponible afin de déterminer si l'allégation semble être fondée et d'établir la portée de l'enquête requise.

**Préjudice** (Injury) – Le préjudice cause un tort. Pour qu'une protection au-delà du niveau de base normal soit envisagée, la compromission de l'information (sa divulgation, destruction, suppression, modification ou interruption non autorisées) doit raisonnablement s'avérer préjudiciable ou dommageable pour le public en particulier ou des intérêts privés visés par une exemption prévue à la Loi sur l'accès à l'information ou à la Loi sur la protection des renseignements personnels. À titre d'orientation, la classification ou la protection est plus exacte et efficace lorsqu'une institution peut faire le lien entre les types d'informations et un effet nuisible déterminé sur les parties touchées qui vont subir les conséquences du préjudice ou dont les intérêts seront brimés. Cela est nettement préférable pour déceler un préjudice général et plutôt vague. Un autre important facteur est la probabilité qu'un préjudice se concrétise. Essentiellement, pour déterminer un préjudice, il faut d'abord décider qu'il

pourrait y avoir un effet nuisible particulier, puis décider que cet effet pourrait raisonnablement se produire si l'information était communiquée. La plupart des exemptions en vertu des deux lois sont fondées sur un critère de préjudice particulier.

**Préjudice élevé** (High degree of injury) - se traduit habituellement par des pertes de vie, l'effondrement de l'ordre public (p. ex. manifestations violentes), la perte de la souveraineté territoriale, la perte irréparable de la confiance de la population, des pertes financières extrêmement importantes ou une grave perturbation de l'économie, la divulgation des sources de renseignements ou des méthodes de collecte de renseignements, de graves dommages à long terme à la conduite des relations internationales et la non disponibilité d'un service essentiel.

**Préjudice en ce qui a trait à l'accès à des informations personnelles** (Injury) – relié à la Loi sur l'accès à l'information. Exception qui détermine l'intérêt précis, public ou privé, qui doit être protégé des préjudices entraînés par la divulgation de renseignements.

**Préjudice en ce qui concerne les biens** (Injury as it relates to assets) - dommage résultant du compromis des biens.

**Préjudice moyen** (Medium degree of injury) - se traduit habituellement par des blessures ou des maladies chez les particuliers, l'incapacité à mener des enquêtes criminelles ou autres obstacles à l'application efficace de la loi, une grave perte de confiance de la part de la population, la compromission de renseignements personnels particulièrement délicats, des pertes financières importantes ou une perturbation importante de l'économie, l'inefficacité des relations internationales ou fédérales-provinciales, une interruption de services qui nuirait sérieusement aux Canadiens. L'interruption du service pourrait compromettre la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens.

**Premier répondant** (First responder) – une personne, comme un policier, un pompier ou un technicien en soins médicaux d'urgence, qui est formé en soins d'urgence et connait diverses procédures d'urgence et qui est prête à se rendre rapidement sur les lieux d'un accident ou d'un sinistre.

**Préparation** (Preparedness) – étape de la gestion des urgences consistant à prendre des décisions et des mesures avant une urgence afin d'être prêt à intervenir efficacement et à gérer les conséquences.

**Preuve de l'identité** (Evidence of identity) − Un document provenant d'une source qui fait autorité et qui confirme l'identité d'une personne.

**Prévention** (Prévention) – Physique, procédural, technique ou contrôles administratifs qui sont destinées à garantir que les individus, les biens, ou de fonctionnement sont protégés contre les dommages dans la mesure du possible.

**Privilège minimum** (Least privilege) – Détermination des autorisations minimales d'accès aux systèmes pour chaque employé afin qu'il assume ses fonctions selon les principes du « besoin de savoir » et de la « séparation des responsabilités ».

**Probabilité** (Likelihood) – nombre de fois où un résultat particulier se produit dans un ensemble donné.

**Problèmes et accidents structuraux et environnementaux** (Structural/environmental issues and accidents) – désignent les incidents relatifs aux structures des bâtiments ou qui résultent d'événements climatiques et engendrent des défaillances, notamment des inondations, des fuites de gaz ou des problèmes d'approvisionnement en eau, etc.

**Processus d'amélioration de la capacité** (Capability improvement process) - approche à l'échelle du gouvernement pour la collecte et l'analyse de données sur l'intervention du gouvernement dans le cadre d'exercices ainsi que d'événements et d'incidents réels.

**Processus de gestion de la continuité** (Continuity management process) – processus exhaustif, stratégique et systématique pour appuyer la définition et l'analyse de tous les services, de l'infrastructure et des interdépendances, et l'élaboration de plans de gestion de la continuité.

**Proférer des menaces** (Uttering threats) – faire des déclarations ou poser des gestes violents, méprisants, menaçants, insultants, offensants ou provocants à l'encontre d'une autre personne.

**Profil d'accès** (Access profile) – privilèges d'accès minimal aux réseaux/systèmes des technologies de l'information (TI) et à l'information de l'Agence, accordés à un employé de l'Agence pour lui permettre d'effectuer les tâches reliées à son travail.

**Programme de planification de la continuité des activités** (Business continuity planning program) –vise à assurer la prestation continue des services indispensables et des biens essentiels qui contribuent à la santé, à la sécurité et au bien-être économique des Canadiens, ainsi qu'au fonctionnement efficace du gouvernement.

**Programme de sécurité** (Security program) – ensemble des moyens mis en œuvre et des activités liés à la sécurité qui sont gérés dans le but de répondre à des besoins particuliers et d'obtenir les résultats prévus.

**Programme ou activité** (Program or activity) – est, aux fins de la collecte, de l'utilisation ou de la communication appropriée de renseignements personnels par des institutions assujetties à cette politique, un programme ou une activité autorisé ou approuvé par le Parlement. L'autorisation parlementaire est habituellement donnée par une loi du Parlement, par un règlement subséquent ou par l'approbation des dépenses envisagées qui sont indiquées dans les budgets des dépenses, puis autorisées par une loi de crédits. Toute activité menée dans le cadre de l'administration de tels programmes entre également dans cette définition.

**Propriétaire de l'application** (Application owner) – propriétaire ou contrôleur de l'application ou du groupe d'applications chargé de mettre en œuvre les règles opérationnelles de gestion de l'information et de faire appliquer et respecter les politiques et les normes de l'ASFC sur le contrôle de l'accès.

Propriétaire de l'information (Information owner) – propriétaire ou contrôleur de l'information responsable de la classification des données ainsi que de la mise en œuvre et de l'exécution des politiques et des normes de l'ASFC régissant le contrôle de l'accès.

**Propriétaires de plates-formes** (Platforms owner) – personnes chargées de définir l'environnement informatique des TI, le soutien aux services d'infrastructure et les exigences en matière de sécurité pour leur plate-forme respective. Les propriétaires de plates-formes peuvent déléguer aux propriétaires de biens la responsabilité d'administrer l'accès, au quotidien.

**Protection** (Protection) – en matière de sécurité matérielle, « protection » désigne le recours à des obstacles matériels, psychologiques et de procédure visant à retarder l'accès non autorisé ou à exercer un effet dissuasif à cet égard, y compris les obstacles visuels et auditifs.

**Protection de base des édifices** (Base building security attributes) - Les mesures de sécurité adoptées par le gardien sont destinées à protéger l'édifice mais non les biens qui y sont conservés. La protection de base des édifices constitue une base ou un point de départ auxquels d'autres exigences (soit la protection de base et les mesures de protection renforcée) viennent se greffer dans le but de protéger les biens particuliers détenus par l'institution.

**Protégé** (Protected) - Cote qui indique que les renseignements répondent à la définition des autres renseignements sensibles et qu'ils nécessitent une protection accrue.

**Protocole relatif à la protection des renseignements personnels** (Privacy protocol) – ensemble de procédures documentées à respecter lors de l'utilisation de renseignements personnels à des fins non administratives, y compris la recherche, les statistiques, la vérification et l'évaluation. Ces procédures visent à faire en sorte que le traitement des renseignements personnels de particuliers soit conforme aux principes de la Loi.

## R

**Raison d'être de l'exercice** (Exercise purpose) – motif justifiant la tenue d'un exercice.

**Rapprochement** (Reconcilliation) – processus consistant à comparer deux ensembles de données ou plus afin de traiter des anomalies et de faire la preuve d'exactitude.

**Ratissage de sécurité** (Security sweep) – désigne l'activité de surveillance la moins officielle qui vise principalement à évaluer le respect des normes de sécurité. Les ratissages comprennent la surveillance périodique du niveau de sécurité d'un secteur opérationnel et ont pour objectif d'assurer le maintien d'un niveau de sécurité acceptable.

**Réacheminement automatique de courriels** (Auto-forward emails) – possibilité de transférer ou de rediriger les courriels automatiquement à une autre adresse électronique sans avoir à les ouvrir au préalable.

**Réaction aux risques** (Risk response) - désigne le continuum de mesures de contrôle ou d'atténuation du risque élaborées ou mises en application pour gérer un risque déterminé.

**Recherche des faits** (Fact-finding) – Ce terme signifie la collecte de tous renseignements se rapportant à une plainte, qui est habituellement effectuée par la gestion locale conformément aux lignes directrices.

**Recommandation** (Recommendation) - plan d'action recommandé appuyant une constatation favorable ou donnant suite à un point à améliorer

**Regroupement** (Aggregation) – situation où un ensemble de biens peuvent être catégorisés à un niveau de sensibilité plus élevé que les parties qui le forment en raison du préjudice accru que pourrait causer toute compromission à ce regroupement de biens. Le regroupement s'applique généralement à la confidentialité, mais, dans certains cas, il peut également concerner la disponibilité, l'intégrité et la valeur.

**Renforcement des cibles** (Target hardening) – constitue la somme de tous les composants inanimés d'un système de sécurité matériel qui protègent (ou renforcent) une cible donnée.

**Renseignement** (Information) – actif ou ressource de l'organisation, défini comme des données, des faits ou des connaissances qui sont enregistrés, peu importe le format, le support d'enregistrement ou la technologie utilisée.

**Renseignement de l'organisation** (Corporate information) – s'entend des renseignements consignés issus des actions, des transactions et des processus opérationnels, des fonctions et des activités de l'ASFC.

**Renseignement de nature délicate** (Sensitive information) – information qui doit être protégée car la divulgation, la modification, la perte, ou la destruction de celle-ci risquerait vraisemblablement de porter préjudice à un intérêt non-national (protégé) ou national (classifié).

**Renseignement défavorable** (Adverse information) – renseignement pouvant constituer un motif raisonnable de croire que la personne peut ne pas se montrer digne de la confiance qu'on lui accordera. Il faut chercher à savoir s'il pourrait voler des objets précieux, utiliser à son profit les biens et renseignements auxquels il aura accès ou ne pas protéger les biens et renseignements, ou se comporter d'une façon qui nuirait à leur protection.

**Renseignement électromagnétique** (SIGINT) – (Signals intelligence) - information technique ou renseignement composé (individuellement ou en combinaison) de renseignement sur les communications (COMINT), de renseignement électronique (ELINT) et de renseignements sur les instruments et les signaux étrangers (FISINT).

**Renseignement électronique** (Electronic intelligence) – information technique ou renseignement tiré de la collecte, du traitement et de l'analyse d'émissions électromagnétiques autres que de communications.

**Renseignement Secret** (Secret information) – renseignement dont la divulgation non autorisée pourrait causer un préjudice grave à l'intérêt national. Exemples : procès-verbaux ou documents du Cabinet, des comités, avant-projets de loi, stratégies et tactiques liées aux négociations internationales, dossiers ayant des répercussions nationales en matière de sécurité.

**Renseignement sur les communications** (COMINT) (Communications intelligence) - information technique ou renseignement tiré de l'exploitation, par une personne autre que le destinataire prévu, de systèmes de télécommunications, de systèmes et de réseaux de technologie de l'information, ainsi que de toute donnée ou information technique véhiculée par ceux-ci, contenue dans ceux-ci ou s'y rapportant.

**Renseignement tiré de signaux d'instrumentation étrangers** (Foreign instrumentation signals intelligence) – information technique ou renseignement tiré de la collecte, du traitement et de l'analyse de signaux d'instrumentation étrangers, par une personne autre que le destinataire prévu.

**Renseignements classifiés** (Classified information) – renseignements d'intérêt national qui concerne la défense et maintenance de la stabilité sociale, politique et économique du Canada, susceptibles d'être visés par une exclusion ou une exception en vertu de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels, et dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national si l'information est compromise.

- Confidentiel (Confidential) – Préjudice à l'intérêt national si compromis (renseignements liés aux négociations avec les provinces, stratégies, tactiques, rapports politiques et économiques sur d'autres pays, non disponibles au Canada).
- Secret (Secret) – Préjudice grave à l'intérêt national si compromis (comptes rendus de réunions ou rapports de décision des comités du Cabinet, avant-projet d'une loi, tactiques relatives aux négociations internationales, dossiers ayant des répercussions sur la sécurité nationale).
- Très Secret (Top Secret) – Préjudice exceptionnellement grave à l'intérêt national si compromis (négociations importantes et significatives, questions extrêmement importantes liées à l'excécution de la loi et aux renseignements, renseignements classifiés par le SCRS et la GRC concernant des activités criminelles ou des menaces pour la sécurité.

**Renseignements de tiers** (Third party information) – aux termes de l'article 20 de la Loi sur l'accès à l'information, les renseignements de tiers comprennent les secrets industriels de tiers, les renseignements financiers, commerciaux, scientifiques ou techniques d'une entreprise dont la divulgation risquerait vraisemblablement de nuire à sa compétitivité ou d'entraver des négociations menées en vue de contrats ou à d'autres fins.

**Renseignements et biens désignés** (Designated information and assets) – renseignements et biens dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt non national et dont la confidentialité, l'intégrité, la disponibilité ou la valeur constituent une garantie de protection. Les biens désignés peuvent comprendre, entre autres, les ordinateurs, les imprimantes, les télécopieurs, l'argent liquide et les éléments négociables.

**Renseignements personnels** (Personal information) – renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment les renseignements relatifs à sa race, à son âge ou à sa situation de famille; les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé; tout numéro identificateur qui lui est propre; ses empreintes digitales; son adresse; ses idées personnelles, etc.

**Renseignements protégés** (Protected information) - renseignements privés, commerciaux et autres que d'intérêt national susceptibles d'être visés par une exclusion ou une exception en vertu de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels et dont la compromission risquerait vraisemblablement de porter préjudice à un particulier ou à une organisation.

- Protégé A (Protected A) : Préjudice léger en cas de compromission. Renseignements dont la communication non autorisée pourrait causer un préjudice à un particulier, à un organisme ou au gouvernement (ingérence dans la vie privée, embarras, etc.).
- Protégé B (Protected B) : Préjudice moyen ou grave en cas de compromission. Renseignements dont la communication non autorisée pourrait causer un grave préjudice à un particulier, à un organisme ou au gouvernement. (traitement préjudiciable; atteinte à la réputation ou perte d'un avantage concurrentiel, etc.).
- Protégé C (Protected C) : Renseignements dont la communication non autorisée pourrait causer un préjudice extrêmement grave à un particulier, à un organisme ou au gouvernement; (importante perte financière ; décès, programme de protection des témoins; renseignements sur un informateur, etc.).

**Renseignements publics** (Public information) – la catégorie publique reconnaît que les renseignements ne revêtent pas un intérêt national, qu'ils ne sont pas de nature délicate (non protégés et non classifiés) et qu'ils ne constituent pas un risque vraisemblable de préjudice. Ils ne requièrent donc aucune mesure de protection.

**Renseignements transitoires** (Transitory information) – renseignements qui sont requis durant une période limitée pour prendre une mesure de routine ou préparer un document ultérieur. Les renseignements transitoires comprennent tout renseignement utilisé dans les communications courantes, les ébauches de documents auxquelles seront ajoutés des commentaires et des renseignements supplémentaires en vue des versions ultérieures, les versions de travail des documents qui n'ont pas été communiqués à l'extérieur du bureau responsable et les copies de documents utilisées uniquement à des fins de référence.

**Réponse** (Response) - réaction lorsque survient un incident ou une urgence afin d'évaluer les dommages ou les répercussions en plus de déterminer le niveau d'intervention sur le plan du contrôle et du confinement requis. La réponse recouvre également les activités relatives aux évacuations et à la sécurité. L'intervention décrit aussi les politiques, les procédures et les mesures à suivre en cas d'urgence.

**Réponse en cas d'urgence** (Emergency Response) - réponse immédiate aux effets de toute urgence, qu'il s'agisse d'évacuer un édifice endommagé, d'éteindre un incendie ou d'arrêter une fuite.

**Représailles** (Reprisal) – désignent toutes les mesures prises à l'encontre d'un fonctionnaire pour le motif qu'il a fait une divulgation protégée ou pour le motif qu'il a collaboré de bonne foi à une enquête menée sur une divulgation ou commencée au titre de l'article 33 (de la Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles)

**Représentant local de la sécurité** (Local security official) – personne qui se voit attribuer des responsabilités au chapitre de la mise en œuvre des politiques, des normes et des procédures en matière de sécurité de l'Agence.

**Reprise** (Recovery) - mise en œuvre des mesures prioritaires nécessaires pour rendre aux processus et aux fonctions de soutien une certaine stabilité opérationnelle, suite à une interruption ou à un sinistre.

**Réseau** (Network) – réseau informatique local ou étendu qui permet la transmission numérique de tous les types de données, lesquelles peuvent être utilisées par l'ensemble du réseau.

**Réseau cryptographique** (Cryptographic network) - réseau de télécommunication (quel qu'en soit la taille ou le nombre d'utilisateurs) dans lequel l'information est protégée au moyen d'équipements cryptographiques compatibles utilisant la même clé.

**Réseau d'accès externe** (External access network) – inter réseau fournissant les services de réseau pour connecter une zone publique.

**Réseau de télécopieurs classifiés** (Secure classified facsimile network) – renvoie à des télécopieurs particuliers liés au dispositif de chiffrement approuvé utilisé pour la transmission des données de niveau Très Secret, au maximum.

**Réseau de télécopieurs protégés** (Secure protected facsimile network) –se réfère aux télécopieurs liés au dispositif de chiffrement approuvé utilisé pour la transmission de données de niveau Protégé B, au maximum.

**Réseau de télécopieurs standards public** (Standard public facsimile network) – désigne les télécopieurs connectés à une ligne téléphonique régulière.

**Réseau électronique** (Electronic Networks) - Groupes d'ordinateurs et de systèmes informatiques qui sont en mesure de communiquer entre eux, y compris, mais sans s'y limiter, Internet, les réseaux de données électroniques du gouvernement du Canada et l'infrastructure de réseau vidéo ainsi que des réseaux publics et privés à l'extérieur d'un ministère. Le réseau comprend les éléments à la fois avec et sans fil.

**Réseau étendu** (Wide Area Network) – réseau situé à l'extérieur d'un pare-feu ou réseau qui fait le lien avec Internet.

**Réseau local** (Local area network) – réseau informatique qui permet d'interconnecter des ordinateurs dans une zone restreinte.

**Réseau local sans fil** (Wireless LAN) – réseau local sans fil qui fait le lien entre deux ordinateurs ou dispositifs, ou plus, sans nécessiter de câbles.

**Réseau privé virtuel** (Virtual private network) – réseau informatique logique à usage restreint qui permet de séparer le trafic sur le réseau, généralement au moyen de la tunnellisation des liens du réseau virtuel sur le réseau réel. La ségrégation peut être virtuelle ou matérielle et utiliser la cryptographie, les contrôles de réseaux, les contrôles d'accès ou la séparation matérielle.

**Réseau sécurisé** (Secure network) – permet de vérifier l'authenticité de tous les points d'extrémité du réseau et de protéger la confidentialité des données transmises entre les points d'extrémité. Les contrôles de confidentialité peuvent comprendre le chiffrement global du trafic de la session (p. ex. couche de sockets sécurisés), le trafic sur le réseau (p. ex. IPSec), ou les liens entre les sites au moyen du chiffrement approuvé par ASFC. Cette méthode permet de transmettre les dossiers entre les points d'extrémité du réseau sans avoir à effectuer de tâches supplémentaires de chiffrement hors ligne.

**Réseaux étendus sans fil** (Wireless Wide Area Networks) – type de réseau sans fil. Le WWAN diffère du WLAN (réseau local sans fil) car il fait appel aux technologies des réseaux cellulaires comme le WIMAX.

**Réseaux personnels sans fil** (Wireless personal area networks) – réseau personnel sans fil de très courte portée, généralement de quelques mètres. Les WPAN peuvent être utilisés pour la communication entre les dispositifs personnels (communication intra personnelle) ou pour la connexion à un réseau supérieur et à l'Internet (liaison montante).

**Résilience** (Resilience) – aptitude d'un système, d'une communauté ou d'une société potentiellement exposé à des risques à s'adapter, en résistant ou en changeant, afin d'atteindre et de maintenir une structure et un niveau de fonctionnement acceptables.

**Responsabilisation** (Accountability) – obligation de démontrer un rendement et d'en assumer à la lumière des engagements et des résultats prévus. Il doit être clair que la reddition de comptes ne correspond pas aux responsabilités, puisque les responsabilités professionnelles peuvent être déléguées à une autre personne ou entité; toutefois l'obligation de rendre des comptes relativement au travail continue de relever de l'entité qui délègue les responsabilités, tout comme l'obligation de rendre des comptes en ce qui concerne la délégation.

**Responsable** (Lead) – secteur ou région demandant la tenue d'un exercice ou organisant un exercice (à l'échelon régional ou des directions générales) avec ou sans l'aide de la Section de la gestion des urgences de la Direction du Centre des opérations frontalières et des grands événements (dans le cas d'un CRPA), ou région ou secteur touché par un événement ou un incident (à l'échelon régional ou des directions générales) qui a une incidence sur les procédures opérationnelles habituelles (dans le cas d'un RAE ou d'un RAI).

**Responsable de la sécurité** (Security official) – personne qui se voit attribuer des responsabilités au chapitre de la mise en œuvre des politiques, des normes et des procédures en matière de sécurité de l'Agence.

**Ressources électroniques** (Electronic resources) – groupes d'ordinateurs, réseaux d'ordinateurs et systèmes, fonctions ou dispositifs attribués aux utilisateurs ou aux programmes. Ces ressources comprennent Internet, les fonctions, les logiciels ou les dispositifs internes à l'ASFC et les fonctions ou les dispositifs publics et privés externes à l'Agence. Elles incluent également le matériel, comme les ordinateurs autonomes, les ordinateurs portatifs, le matériel périphérique, les dispositifs de mémoire, les dispositifs sans fil et tous autres moyen utilisé pour obtenir, stocker ou diffuser de l'information. Beaucoup de dispositifs non informatiques comme les appareils photo numériques et les téléphones cellulaires sont considérés comme étant des ressources électroniques en raison de leur capacité de stockage et de diffusion de l'information.

**Rétablissemen**t (Recovery) – Rétablissement Mesures prises pour restaurer ou rétablir les conditions à un niveau acceptable après une catastrophe.

**Revue de sécurité** (Security review) – évaluation locale de la mise en œuvre des politiques, des normes et des procédures de l'Agence en matière de sécurité.

**Risque** (Risk) – il s'agit de la possibilité qu'une vulnérabilité soit exploitée. Dans le contexte du SCT, le risque s'entend également de l'incertitude qui peut engendrer l'exposition à des événements ou résultats non désirés. Il s'agit de l'expression de la probabilité et de l'incidence d'un événement susceptible de nuire à la réalisation des objectifs d'une organisation.

**Risque lié à l'identité** (Identity risk) – Le risque lié à l'identité est le risque qu'une personne, une organisation ou un appareil ne soit pas celui qu'il prétend être.

**Risque lié aux justificatifs** (Credential risk) − Le risque qu'une personne, une organisation ou un appareil ait perdu le contrôle du justificatif qui lui a été délivré.

**Risque résiduel** (Residual risk) – Niveau de risque restant après avoir pris en considération les mesures d'atténuation des risques et les contrôles en place.

**Rootkit** (Rootkit) – Il s'agit d'un type de logiciel malveillant furtif conçu pour rendre certains processus ou programmes indétectables par les méthodes normales de détection et permettant un accès privilégié continu à un ordinateur.

# S

**Sans fil** (Wireless) – désigne toute technologie qui communique par interface aérienne, comme les fréquences infrarouges ou radio, au lieu de suivre des circuits fermés de câblage. Le terme sans fil comprend tous les dispositifs, systèmes, et services qui font appel à des capacités de connectivité sans fil.

**Santé et sécurité** (Health and Safety) – mise en œuvre d'un programme pour garantir un milieu de travail sûr et sain aux employés. Exigé en vertu de l'article 11 du Code canadien du travail.

**Scénarios sur les conséquences** (Consequence scenarios) – scénarios conçus pour simuler toute une gamme de répercussions possibles d'urgence sur l'organisation. Ils sont utilisés pour fournir le contexte dans lequel s'inscrit l'ensemble des initiatives de planification de gestion de la continuité.

**Séance de rétroaction immédiate** (Hot wash) – séance de compte rendu qui se déroule immédiatement après un exercice, un événement ou un incident et qui offre l'occasion aux personnes concernées d'en discuter et de cerner les aspects positifs et négatifs de la gestion et du déroulement de l'exercice, de la gestion de l'événement ou de la réponse à l'incident.

**Sécurisé** (Secure) – état auquel parvient une organisation qui fonctionne à un niveau acceptable de risque résiduel, ou en dessous, auquel on est parvenu en appliquant des pratiques fiables de manière équitable et systématique.

**Sécurité accrue** (Enhanced security) – niveau de sécurité excédant les normes de base acceptées (voir aussi Mesure de protection accrue).

**Sécurité de l'information** – (Information security) mesures de protection physique, technique, procédurale et psychologique appliquées à l'information (sous toutes ses formes), de la conceptualisation de l'information de nature délicate à sa destruction définitive et irrévocable. afin de protéger les ressources d'information et de garantir l'efficacité et l'uniformité des mesures prises en matière de confidentialité, d'intégrité, d'accessibilité, d'autorisation et d'authentification.

**Sécurité de l'immeuble de base** (Base building security) - mesures de sécurité fournies par le ministère gardien afin de protéger un immeuble, mais non les biens qu'il contient. La sécurité de l'immeuble de base établit le fondement ou le point de départ d'autres exigences de sécurité (c.-à-d., mesures de protection minimales et accrues) à ajouter afin de protéger les biens particuliers détenus par l'Agence.

**Sécurité des technologies de l'information** (TI) (Information technologry IT security) - Le programme de mesures collectives fondées sur les politiques et les procédures approuvées, qui protègent les plateformes technologiques sous-jacentes ainsi que les services, les réseaux et les applications qui permettent de recueillir, de traiter, de stocker ou de communiquer des biens d'information.

**Sécurité matérielle** (Physical security) –mesures de sauvegarde matérielle pour empêcher ou retarder l'accès non autorisé aux biens, pour détecter l'accès non autorisé recherché et obtenu et pour déclencher une intervention appropriée.

**Sécurité personnelle** (Personnel security) – fait référence au maintien des normes de conduite appropriées et à l'examen lié à la fiabilité et à l'évaluation de la loyauté visant à déterminer la cote de sécurité requise (p. ex. Fiabilité, Secret et Très secret) pour toutes les personnes qui ont accès aux infrastructures de l'Agence (installations, biens, information, systèmes, etc.).

**Séminaire d'orientation** (Orientation seminar) – exercice axé sur la discussion au cours duquel on explique aux participants les politiques, les plans et les procédures. Il s'agit d'une séance de discussion en groupe, dans un contexte sans stress et où il y a peu ou pas de mise en situation.

**Sensibilisation à la sécurité** (Secuity awareness) – désigne les pratiques, technologies et services utilisés pour promouvoir la sensibilisation, la formation et la responsabilité des utilisateurs en ce qui a trait aux risques de sécurité ainsi qu'aux vulnérabilités, aux méthodes et aux procédures liés aux ressources en technologie de l'information.

**Séparation des tâches** (Segregation of duties) –répartition des tâches liées à un processus entre différentes personnes afin de réduire la portée des erreurs et de la fraude.

**Service** (Service) - Extrant final précis qui comble un ou plusieurs besoins d'un bénéficiaire visé et qui contribue à l'obtention d'un résultat.

**Service de courrier diplomatique** (Diplomatic mail service) – service du ministère des Affaires étrangères, du Commerce et du Développement visant à permettre un échange sûr avec des missions à l'étranger, par valise diplomatique, de renseignements non classifiés, protégés ou classifiés dont il a la responsabilité.

**Service de soutien essentiel** (Critical support service) − Il s'agit d'une politique ou d'un service intra ministériel ou interministériel qui appuie un service essentiel.

**Service essentiel** (Essential service) – service, installation ou activité du gouvernement du Canada qui est ou sera, à tout moment, nécessaire pour assurer la sécurité du public ou d'un segment de la population.

**Service essentiel** (Critical Service) – Service dont la compromission, du point de vue de la disponibilité ou de l'intégrité, porterait un grave préjudice à la santé, à la sécurité ou au bien-être économique des Canadiens, ou encore au fonctionnement efficace du gouvernement du Canada.

**Service prioritaire sans fil** (SPSF) (Wireless Priority Service) – le SPSF est un service mobile de base amélioré qui permet de mettre en attente les appels des employés essentiels inscrits pour qu'ils aient accès au prochain canal de service disponible, tout en réduisant au minimum les répercussions sur l'accès des autres consommateurs à la même infrastructure sans fil.

**Services à large bande mobile** (Mobile broadband) – nom utilisé pour décrire divers types d'accès Internet sans fil haute vitesse au moyen d'un modem portatif, d'un téléphone ou d'un autre dispositif.

**Services de sécurité** (Security services) – Un service qui assume ou appuie directement une fonction de sécurité. Sont exclus les services administratifs généraux.

**Services de soutien internes** (Internal support services) – Services administratifs qui appuient un ministère ou un organisme, ou un programme. Ils ne comprennent pas les services offerts au public ou les autres services directs servant à l'exécution des programmes.

**Services répondant aux normes de sécurité du personnel** (Appropriately-screened services) – Dans le contexte de la transmission, il s'agit de services de messagerie qui œuvrent à contrat pour le GC et dont le personnel détient une cote de fiabilité, comme l'exige la PGS, de niveau correspondant au degré de sensibilité des renseignements dont il a la responsabilité.

**Signalement des incidents de sécurité** (Security incident reporting) – identification, enquête, comptes rendus, traitement et analyse des évènements associés à des violations de la sécurité, à la perte ou à la détérioration des biens, à la confidentialité, à l'intégrité ou à l'accessibilité, et à la valeur relative ou à la confiance du public accordée aux employés de l'Agence, aux biens de nature délicate ou aux opérations.

**Signature numérique** (Digital signature) – méthode visant à authentifier l'information numérique. Les signatures numériques ressemblent aux signatures ordinaires sur papier mais sont créées au moyen de techniques provenant du domaine de la cryptographie à clé publique.

**Sommaire** (Executive summary) – version condensée du Compte Rendu Post Action/Compte Rendu Post Événement/Compte Rendu Post Incident, conçu pour fournir un bref aperçu du rapport (p. ex. les principales observations et les recommandations), qui n'excède pas deux pages. Prévu pour présenter un résumé de l'exercice, de l'événement ou de l'incident à un public qui n'a pas forcément le temps de lire le rapport au complet.

**Source faisant autorité** (Authoritative source) – Il s'agit d'une source qui peut établir des exigences minimales que l'Agence doit respecter.

**Source fiable** (Reliable source) - source de renseignements ou d'un fond de données jugée être exacte et à jour, à laquelle on peut faire confiance lorsqu'il s'agit de valider des renseignements personnels.

**Source générale** (Open source) – fait référence aux renseignements et aux données accessibles au grand public dont l'accès ne nécessite pas de nom d'utilisateur ou de mot de passe.

**Sous double pli cacheté** (Double sealed envelope) – enveloppe scellée (enveloppe intérieure) dûment adressée comportant une cote de sécurité et incluant une note d'envoi et reçu dans l'enveloppe intérieure, laquelle est insérée dans une autre enveloppe scellée (enveloppe extérieure). L'enveloppe extérieure est uniquement adressée et ne comporte pas de cote de sécurité. L'enveloppe intérieure est aussi scellée avec du ruban indécachetable.

**Sous-compte COMSEC** (COMSEC sub-account) - Entité administrative à laquelle a été attribué un identificateur du Système de gestion électronique des clés (autrement dit, un numéro de compte COMSEC) et qui a été établie par un compte COMSEC pour aider à contrôler le matériel COMSEC porté au compte COMSEC.

**Stratégie de mesures de protection** (Safeguarding stategy) – mesures de sécurité mises de l'avant à la suite d'une évaluation de la menace et des risques pour assurer la protection des employés, des renseignements et des autres biens.

**Subornation/acceptation de paiements de facilitation** (Bribery / accepting facilitation payments) – offre, promesse, don, acceptation ou sollicitation d'un avantage pour inciter à commettre une action illégale, contraire à l'éthique ou qui constitue un abus de confiance. Les incitatifs peuvent prendre la forme de cadeaux, de prêts, d'indemnités, de récompenses ou d'avantages divers (taxes, services, dons, etc.).

**Support amovible** (Removable media) – supports qui peuvent servir de mémoire secondaire ou de mémoire d'extension pour un ordinateur, mais qui peuvent aussi être facilement retirés et utilisés comme dispositifs de stockage par exemple, les clés USB, les CD/DVD et les disques durs externes.

**Support électronique** (Electronic media) - tout support qui fait appel à l'électronique ou à l'énergie électromécanique pour permettre à l'utilisateur final d'accéder au contenu.

**Surveillance** (matérielle) (Monitoring) – processus consistant à vérifier, à examiner ou à valider la comptabilisation des biens à intervalles précis.

**Surveillance** (Monitor) – processus de vérification constante de l'activité dans les réseaux et les systèmes en vue de déceler toute activité anormale, illicite, inappropriée, criminelle ou inhabituelle.

**Surveillance (TI)** (Monitoring (IT) – processus de vérification constante de l'activité dans les réseaux et les systèmes pour déceler toute activité anormale, illicite, inappropriée, criminelle ou inhabituelle.

**Surveillance contre contrôle d'accès** (Monitor versus screen access) – surveiller l'accès fournit une surveillance de sécurité et réponds aux perturbations au niveau du périmètre et dans les parties communes de l'établissement. Accès à l'écran - fournit une identification et contrôle service au nom du locataire (par exemple, en examinant les pièces d'identité, demander aux personnes de signer à l'entrée de l'établissement, etc.)

**Surveillance des courriels** (Monitoring of e-mail) – toute mesure liée à l'enregistrement et l'analyse subséquente des activités ou de l'utilisation des services, tel que cela est défini dans cette politique et dans la Politique sur l'utilisation des ressources électroniques de l'ASFC.

**Surveillance des ressources électroniques** (Monitoring of electronic resources) – enregistrement et analyse de l'utilisation des ressources électroniques à des fins opérationnelles et pour évaluer le degré de conformité à la politique gouvernementale.

**Surveillance du renseignement sur les communications** (Communications intelligence control) – administration et coordination des services de soutien à la clientèle pour mener des activités de gestion et de mise à jour. Cotes de sécurité cloisonnées; sécurité et intégrité de la zone d'accès réservé SIGINT (ZARS) et matériel spécial du renseignement.

**Surveillé** (Monitored) – faisant l'objet de guet ou de detection d'infraction à la sécurité.

**Surveillé continuellement** (Monitored Continuously) – faisant l'objet de confirmation sur une base continuelle qu'il n'y a pas eu infraction à la sécurité, comme un système de détection électronique de l'intrusion ou quelqu'un qui garde un point particulier sur une base constante.

**Surveillé sur une base périodique** (Monitored periodically) – faisant l'objet de confirmation sur une base régulière qu'il n'y a pas eu infraction à la sécurité. La fréquence et la diligence de la surveillance sont basées sur les recommandations d'une évaluation de la menace et des risques, comme une patrouille de surveillance ou des employés qui travaillent sur les lieux.

**Système de chiffrement à clé publique** (Asymmetric cryptography) – système de chiffrement faisant appel aux biclés.

**Système de commandement en cas d'incident** (Incident command system) – Il s'agit d'un concept normalisé de gestion des urgences sur place qui est spécialement conçu pour permettre aux utilisateurs d'adopter une structure organisationnelle intégrée correspondant à la complexité et aux exigences d'un ou de plusieurs incidents, et ce, sans être gêné par des limites de compétence.

**Système de défense contre les intrusions** (Intrusion defence system Technologie qui décèle, signale et, si possible, prévient le comportement TI malveillant ou anormal.

**Système de gestion des risques des utilisateurs privilégiés** (Privileged user risk management system) – outil en ligne qui permet de gérer le flux des demandes de GRUP, du demandeur initial (auteur de la demande), à l'autorisation de la direction (superviseur et gestionnaires de niveau 3), en passant par les coordonnateurs, divers administrateurs de GRUP (propriétaires de plates-formes et de biens) et les zones de sécurité, au besoin, tout en tenant les intervenants informés de l'état de la demande.

**Systèmes de technologie de l'information (TI)** (Information technology systems) – champs du traitement des données électroniques, des télécommunications et des réseaux électroniques et leur convergence dans les systèmes; applications, logiciels et matériel connexes ainsi que leur interaction avec des personnes et des machines.

**Systèmes essentiels** (Critical systems) –. Système dont la compromission en termes de disponibilité ou d'intégrité résulterait en un préjudice élevé à la santé, à la sécurité ou au bien-être économique des Canadiens ou encore à l'efficacité du gouvernement du Canada.

**Systèmes primaires** (Primary systems) – désignent les bases de données comme les SAE, les applications sur ordinateur central et les applications sur réseau. Ne sont fournis qu'aux fins des activités de l'Agence.

**Systèmes secondaires** (Secondary systems) – désignent les applications, notamment le courriel, Microsoft Office et Internet (dont l'utilisation personnelle limitée est autorisée).

## T

**Technologie sans fil** (Wireless technology) – technologie qui permet le transfert de renseignements à distance sans utiliser de conducteurs électriques perfectionnés (fil).

**Technologies de l'information** (Information Technology) – les technologies de l'information désignent tout équipement ou système utilisé pour l'acquisition, le stockage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, la commutation, les échanges, la transmission ou la réception automatique de données ou d'information. Elles englobent la conception, le développement, l'installation et la mise en œuvre de systèmes et d'applications informatiques visant à répondre à des besoins opérationnels.

**Télécommunications** (Telecommunications) – désigne toute transmission, émission ou réception de signes, de signaux, d'inscriptions, d'images, de sons ou de renseignements de quelque nature que ce soit, par câble ou radio, par système visuel ou par tout autre système électromagnétique. Cela comprend le téléphone, le télégraphe, le téléimprimeur, la télécopie, la transmission de données, la télévision en circuit fermé et la dictée à distance.

**Téléconférence** (Teleconferencing) – participation à une conférence ou à une réunion à distance à l'aide du système téléphonique.

**Télétravail** (Telework) – concept qui s'applique aux utilisateurs de l'ASFC qui travaillent à partir d'un endroit à distance approuvé (p. ex. domicile ou emplacements à distance) ou qui travaillent souvent en déplacement en utilisant un ordinateur portatif d'accès à distance protégé.

**Témoin** (Witness) – personne autre que l'intimé qui est interrogé aux fins d'obtenir de l'information comportant de la documentation liée à une enquête.

**Tempest** (Tempest) – domaine traitant de la suppression de signaux électromagnétiques émis ou transmis involontairement, qui révèlent des renseignements.

**Temps d'arrêt maximal admissible** (Maximum allowable downtime) – durée maximale Durant laquelle un service peut être non disponible ou être altéré avant qu'en résulte un préjudice moyen u significatif. Pour les services qui doivent être assurés de manière ininterrompue, la valeur de ce paramètre est nulle.

**Terrorisme** (Terrorism) – emploi illégal ou menace d'emploi illégal de la force ou de la violence contre des personnes ou des biens, afin de contraindre ou d'intimider les gouvernements ou les sociétés dans le but d'atteindre des objectifs politiques, religieux ou idéologiques.

**Tolérance au risque** (Risk tolerance) - désigne la volonté d'une organisation d'accepter ou de rejeter un niveau donné de risque résiduel (exposition). La tolérance au risque peut varier au sein d'une organisation, mais elle doit être bien comprise par les personnes qui prennent des décisions relatives aux risques dans un dossier en particulier. Il faut que la tolérance au risque soit claire à tous les niveaux de l'organisation afin de favoriser une prise de décisions éclairée par l'analyse du risque et le recours à des approches tenant compte du risque.

**Transfert sécurisé de dossiers** (Secure file transfer) – les dossiers contenant des renseignements de nature sensible comme les données des partenaires sont chiffrés au moyen du chiffrement hors ligne approuvé par l'ARC afin de protéger leur caractère confidentiel. Cette méthode garantit la protection des dossiers et leur transfert sûr dans un lien de réseau non chiffré. Le chiffrement hors ligne relève de la responsabilité de l'utilisateur final.

**Transmission** (Transmittal) – acheminement de renseignements protégés ou classifiés d'une personne à une autre ou d'un lieu à un autre par un tiers qui n'a pas besoin de connaître les renseignements en question.

**Transmission à l'étranger** (Transmittal outside Canada) – fait de transmettre des renseignements à destination, en provenance ou au sein d'installations du GC (c.-à-d. ambassades, missions ou déploiements, immeubles abritant des ministères ou des organismes, consulats) se trouvant à l'étranger.

**Transmission des renseignements sensible** (Transmittal of sensitive information) - envoyer des renseignements protégés et classifiés d'une personne ou d'un lieu à un autre par l'entremise d'un tiers. Le détenteur n'a pas le besoin de connaître.

**Transporter des renseignements sensible** (Transport of Sensitive Information) - apporter avec soi des documents protégés et classifiés pour les remettre à une autre personne ou les déposer à un autre endroit. La personne qui transporte les documents (renseignements) doit en avoir véritablement besoin (principe d'accès sélectif).

**Transporteur cautionné** (Bonded carrier) – transporteur ayant déposé une garantie auprès de l'ASFC et qui est autorisé à transporter, sous le contrôle de l'Agence, entre divers points au Canada, des marchandises assujetties à des droits de douane pour lesquelles les droits n'ont pas encore été payés.

**Très secret** (Top Secret) – niveau s'appliquant aux renseignements pour lesquels la compromission pourrait causer un préjudice extrêmement grave à l'intérêt national du Canada. Exemples : négociations importantes et de grande envergure, questions extrêmement importantes liées à l'exécution de la loi et au renseignement, information classifiée par le SCRS et la GRC qui a trait aux plans stratégiques ainsi qu'aux menaces criminelles ou liées à la sécurité.

## U

**Urgence** (Emergency) Dans le contexte des activités du gouvernement, une urgence fait référence à un événement, d'origine interne ou externe, réel ou imminent qui, du fait de ses effets nocifs et de son caractère imprévisible ainsi que de la nécessité d'intervenir sur-le-champ pourrait faire en sorte que l'organisation visée modifie en partie ou en totalité la façon dont elle s'acquitte de ses autres responsabilités. Une urgence sera généralement une situation anormale qui exige une réponse immédiate allant au-delà des procédures normales, afin de limiter les dommages causés aux personnes, aux biens et à l'environnement.

**Usage compatible** (Consistent use) - usage se rapportant de façon raisonnable et directe à l'objectif premier pour lequel les renseignements ont été obtenus ou recueillis. Cela signifie que les fins premières et les fins qui ont été proposées sont si intimement liées que la personne s'attendrait à ce que les renseignements soient utilisés pour les fins conformes, même si elles n'ont pas été expressément mentionnées.

**Usage de drogue/substance intoxicante** (Drug/intoxicant usage) – la définition précise l'interdiction mais ne définit pas nécessairement les termes employés. Suggestion : consommation de toute substance considérée comme étant illégale ou contrevenant au code de conduite de l'ASFC, pendant le service, en uniforme (en service ou non), lors de la conduite d'un véhicule officiel ou sur les lieux où l'ASFC mène ses activités.

**Usage de force excessive** (Excessive use of force) – usage d'un niveau de de force excédant le niveau qui est de mise dans une situation donnée. Les employés autorisés à faire usage de la force doivent limiter le recours à la force à un niveau qui est adapté à la situation. Tout débordement est considéré comme un usage de force excessive.

**Utilisateurs privilégiés** (Privileged user) – utilisateurs qui, de par leurs fonctions ou rôles, se voient conférer des pouvoirs pour administrer un système de technologie de l'information qui sont supérieurs à ceux que détiennent la plupart des utilisateurs. Il existe trois catégories d'utilisateurs privilégiés : 1) personnel de soutien et d'administration des systèmes de TI; 2) personnel de développement des systèmes; 3) autre personnel d'administration et de sécurité.

**Utilisation interdite** (Prohibited usage) - actes criminels, infractions à des lois fédérales et provinciales non pénales à caractère réglementaire et actions qui rendent une personne autorisée ou un établissement passible de poursuites au civil. De telles activités peuvent exposer le réseau d'un ministère à des attaques ou à des exploitations malveillantes.

# V

**Valeur** (Value) – valeur approximative, soit monétaire, culturelle, intellectuelle ou autre.

**Vandalisme contre des biens de l'ASFC** (Vandalism of CBSA property) – dommage causé à une installation ou à des biens de l'ASFC, sans aucune entrée par la force (p. ex. fenêtres ou lumières brisées, graffitis, etc.).

**Ver informatique** (Worm) - un ver informatique est un maliciel indépendant qui se copie afin de se répandre dans d'autres ordinateurs. Contrairement au virus, il n'a pas besoin de se joindre à un programme déjà installé. Les vers causent presque toujours certains dommages au réseau.

**Vérification** (Programme) - fonction d'évaluation professionnelle indépendante, qui produit des conclusions objectives et corroborées sur la conception et le fonctionnement des processus de gestion des risques, de contrôle et de gouvernance de l'organisation.

**Vérification** (Sécurité matérielle) – vérification que les contrôles de sécurité matérielle administratifs, physiques, de procédure et techniques sont parvenus à employer des moyens adaptés et que ces contrôles satisfont aux exigences à tous les stades de leur cycle de vie ou de leur application. Les normes applicables à la réalisation des vérifications sont extraites de l'Association internationale des auditeurs internes, tel que les a acceptées le Secrétariat du Conseil du Trésor du Canada (SCT).

**Vérification de compte COMSEC** (COMSEC account audit) – examen coopératif indépendant des dossiers et des activités d'un compte COMSEC dans le but d'assurer que le matériel COMSEC produit par le compte COMSEC, ou confié à ce dernier, est manutentionné et contrôlé conformément à la directive applicable.

**Vérification de l'inventaire** (Inventory Verification) – contrôle visant à déterminer la présence de tous les éléments et leur comptabilisation dans les différents systèmes comptables d'une organisation.

**Vérification du dossier de police** (Law enforcement record check) – vérification effectuée par la GRC dans diverses bases de données contenant des informations de police.

**Vérification nominale du casier judiciaire** (Criminal record name checks) – recherche effectuée pour déterminer si une personne a une condamnation au criminel pour laquelle elle n'a pas obtenu de réhabilitation. Ces vérifications sont faites en consultant le répertoire national des casiers judiciaires de la Gendarmerie royale du Canada (GRC).

**Vidéoconférence** (Video conferencing) – participation à distance à une conférence ou à une réunion à l'aide d'un système de caméra vidéo (et non par Internet ou intranet).`

**Vie privée** (Privacy) - droit d'un individu à son intimité et à être protégé contre toute intrusion injustifiée. Il s'agit aussi du droit d'un individu de garder le contrôle de ses renseignements personnels et de savoir à quelles fins ils sont utilisés, divulgués et où ils sont conservés.

**Violence en milieu de travail** (Workplace violence) – acte, conduite, menace ou geste qui risquerait vraisemblablement de causer un dommage, une blessure ou une maladie à un employé en milieu de travail.

**Virus informatique** (Computer virus) – un virus informatique est un type de maliciel qui, lorsqu'exécuté, se copie dans d'autres programmes ou dossiers de données informatiques et réalise une activité donnée qui s'avère préjudiciable pour les systèmes infectés.

**Visiteur** (Visitor) – une personne qui ne travaille pas pour le ministère ou l'organisation du gouvernement, occupant l'établissement ou le complexe hôte, et qui a une raison légitime d'être sur les lieux et qui doit faire l'objet d'une vérification par le système de contrôle d'accès en vigueur.

**Voies de fait** (Assault) – (Tiré du Code criminel, article 265.1) Commet des voies de fait, ou se livre à une attaque ou une agression, quiconque, selon le cas :

a) d'une manière intentionnelle, emploie la force, directement ou indirectement, contre une autre personne sans son consentement;
b) tente ou menace, par un acte ou un geste, d'employer la force contre une autre personne, s'il est en mesure actuelle, ou s'il porte cette personne à croire, pour des motifs raisonnables, qu'il est alors en mesure actuelle d'accomplir son dessein;
c) en portant ostensiblement une arme ou une imitation, aborde ou importune une autre personne ou mendie.

**Voix sur le protocole Internet** (Voice over Internet protocol) – conversation individuelle sur Internet.

**Vol** (Theft) – acte criminel qui consiste à s'emparer des biens d'une autre personne sans son consentement.

**Vol d'identité** (Identity theft) – usurpation délibérée de l'identité d'une autre personne. Se produit lorsque quelqu'un vole votre nom et d'autres renseignements personnels, à votre insu. Le vol d'identité vise généralement des fins frauduleuses (avoir accès aux ressources financières d'une personne ou commettre un acte criminel).

**Vol de détournement** (Diversion theft) - vol de détournement est un "con" exercé par les voleurs professionnels, normalement contre une entreprise de transport ou de messagerie. L'objectif est de persuader les personnes responsables de la prestation légitime de marchandises que les marchandises sont priées ailleurs.

**Vol qualifié** (Robbery) – désigne l'action de prendre de l'argent, un bien personnel ou un autre article de valeur qui appartient à une autre personne contre son consentement et avec violence ou menace de violence.

**Vulnérabilité** (Vulnerability) – une insuffisance en matière de sécurité qui pourraient augmenter la susceptibilité à faire des compromis ou des blessures.

# W

**Wi Fi** (technologie Wi-Fi) – nom commercial populaire de la technologie sans fil utilisée pour les réseaux domestiques, les téléphones cellulaires et les jeux vidéo, entre autres.

# Z

**Zone** (zone) – série d'espaces clairement visibles pour contrôler progressivement l'accès.

**Zone d'accès public** (Public Zone) - Tout ce qui entoure une installation gouvernementale, auquel le grand public a accès. On ne doit jamais y traiter de renseignements sensibles.

**Zone d'accueil** (Reception zone) - l'espace entre une zone d'accès public et une zone de travail. Cette zone est généralement située à l'entrée d'une installation et c'est là que, pour le public, il y a la première mesure de sécurité matérielle, comme des portes et d'autres obstacles matériels (p. ex. des

tourniquets). L'accès du public peut être limité à certaines heures de la journée ou pour des raisons précises. Une entrée située au delà de la zone d'accueil est indiquée par un périmètre facile à reconnaître : porte ou meubles disposés d'une certaine façon, ou paravents dans une aire ouverte. Les biens ou les renseignements du ministère ne doivent jamais être entreposés ou laissés sans surveillance dans cette zone.

**Zone d'accès public** (Public-access zone) – lieu qui entoure habituellement un immeuble gouvernemental ou en fait partie. Exemples : les terrains entourant un immeuble et les corridors publics, ainsi que les vestibules d'ascenseur dans des immeubles à plusieurs occupants.

**Zone d'accès réservé SIGINT ou local isolé pour matériel spécial** (LIMS) (SIGINT Secure Area (SSA) or Sensitive Compartmented Information Facility (SCIF) – terme désignant une pièce sécuritaire ou un centre de données qui empêche la surveillance électronique et prévient la fuite de données. Un LIMS utilise des méthodes passives comme une pièce entourée d'une gaine en métal hermétiquement fermée (cage de Faraday) et des méthodes actives (brouillage).

**Zone de sécurité** (Security Zone) – zone dont l'accès est réservé au personnel autorisé ainsi qu'aux visiteurs autorisés qui sont escortés. Des renseignements protégés C, Secrets et Très Secrets peuvent y être traités, mais doivent être entreposés dans un coffre de sûreté ou un classeur verrouillable approuvé. Ils doivent également être surveillés en tout temps.

**Zone de sécurité des technologies de l'information** (Information technology security zone) – environnement réseau possédant des limites bien définies, une administration de la sécurité et un niveau normalisé de vulnérabilité aux menaces visant le réseau. On distingue les types de zones de sécurité des TI d'après les exigences en matière de sécurité qui s'appliquent aux interfaces, au contrôle du trafic, à la protection des données, au contrôle de la configuration de l'hôte (dispositif) et au contrôle de la configuration de réseau.

**Zone de sécurité des TI** (IT Security Zones) – environnement réseau possédant des limites bien définies, une administration de la sécurité et un niveau normalisé de vulnérabilité aux menaces visant le réseau

**Zone de travail** (Operations zone) – secteur dont l'accès est limité au personnel qui y travaille et aux visiteurs accompagnés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée sur une base périodique. Exemple : un espace à bureaux à aire ouverte typique.

**Zones d'accès restreint** (Restricted access area) (zone restreint– zones d'opérations où l'accès est limité aux personnes autorisées, incluant les zones de travail, de sécurité et de haute sécurité.

**Zones restreintes** (Restricted zone) – inclut les zones de travail, les zones de sécurité et les zones de haute sécurité. Voir la définition de Zones.